高等学校信息安全专业指导性专业规范

教育部高等学校信息安全专业教学指导委员会 编制

Information Security

清华大学出版社

高等学校信息安全专业指导性专业规范

教育部高等学校信息安全专业教学指导委员会　编制

清 华 大 学 出 版 社

北　京

内 容 简 介

本书主要介绍我国制定的第一个"高等学校信息安全专业指导性专业规范"。指导性专业规范是国家教学质量标准的一种表现形式。指导性专业规范是国家对本科教学质量的最低要求，主要规定本科学生应该学习的基本理论、基本技术和基本应用。不同层次的学校在这个最低要求的基础上增加本学校的要求，制订本学校的教学质量标准，体现本学校的办学定位和办学特色。

围绕"高等学校信息安全专业指导性专业规范"，本书首先对信息安全学科进行了讨论，给出了其内涵、主要研究内容和研究方向、理论基础和方法论基础等重要内容。在此基础上详细给出了我国制定的第一个"信息安全专业指导性专业规范"的具体内容。然后针对规范给出了其课程体系和实践能力教学体系的示例。最后作为率先全面应用规范的实例，以附录形式列出了武汉大学信息安全专业的课程体系、实践教学体系及其教学计划，供大家参考。

本书可供信息安全专业的教师、学生和教学管理人员用作教学参考书，也可供信息类其他专业的教师、学生和教学管理人员用作教学参考书，还可供信息领域的科学技术人员用作参考书。

图书在版编目(CIP)数据

高等学校信息安全专业指导性专业规范/教育部高等学校信息安全专业教学指导委员会编制. --北京：清华大学出版社，2014
ISBN 978-7-302-35721-6

Ⅰ. ①高…　Ⅱ. ①教…　Ⅲ. ①信息安全－高等学校－教学参考资料　Ⅳ. ①TP309

中国版本图书馆 CIP 数据核字(2014)第 060826 号

责任编辑：张　民　薛　阳
封面设计：
责任校对：李建庄
责任印制：

出版发行：清华大学出版社
网　　址：http://www.tup.com.cn，http://www.wqbook.com
地　　址：北京清华大学学研大厦 A 座　　**邮　　编：**100084
社 总 机：010-62770175　　**邮　　购：**010-62786544
投稿与读者服务：010-62776969，c-service@tup.tsinghua.edu.cn
质量反馈：010-62772015，zhiliang@tup.tsinghua.edu.cn
课件下载：http://www.tup.com.cn，010-62795954
印 刷 者：
装 订 者：
经　　销：全国新华书店
开　　本：180mm×235mm　　**印　　张：**11　　**字　　数：**162 千字
版　　次：2014 年 4 月第 1 版　　**印　　次：**2014 年 4 月第 1 次印刷
印　　数：1～　000
定　　价：　.00 元

产品编号：032389-01

教育部“高等理工教育教学改革与实践项目”——“信息安全专业指导性专业规范研制”项目组成员

张焕国	教授	武汉大学
王小云	教授	山东大学
方　勇	教授	北京电子科技学院
杨义先	教授	北京邮电大学
王清贤	教授	解放军信息工程大学
刘建伟	教授	北京航空航天大学
张宏莉	教授	哈尔滨工业大学
秦玉海	教授	中国刑事警察学院
秦志光	教授	电子科技大学
来学嘉	教授	上海交通大学
张　民	副编审	清华大学出版社

特邀专家：

李　晖	教授	西安电子科技大学
贾春福	教授	南开大学

《高等学校信息安全专业指导性专业规范》主要执笔人员

张焕国	教授	武汉大学
杜瑞颖	教授	武汉大学
傅建明	教授	武汉大学
赵　波	教授	武汉大学
王丽娜	教授	武汉大学

注：武汉大学计算机学院信息安全系的许多老师都参与了这项工作，在此向他们致谢！

《高等学校信息安全专业指导性专业规范》评审意见

2012 年 11 月 2 日，教育部高等学校信息安全类专业教学指导委员会受教育部委托，在天津组织《高等学校信息安全专业指导性专业规范》（以下简称《规范》）评审会。会议听取了“信息安全专业指导性专业规范研制”项目组的《规范制订工作报告》、《规范内容设计报告》和《规范应用报告》。经质询和讨论后评审专家组认为：

（1）我国信息安全专业的办学规模发展迅速，为了确保信息安全专业办学质量，迫切需要一个指导信息安全专业办学的规范。根据教育部的要求，由 11 所高校专家组成的项目组历时 5 年制定出我国第一个《高等学校信息安全专业指导性专业规范》。又经过许多学校两年多的试用和进一步的修改，形成了提交给本次会议的规范文本。这一规范对指导、规范我国信息安全专业的办学和提高办学质量具有重要的意义。

（2）《规范》对信息安全学科的内涵、理论基础、方法论基础、主要研究方向和研究内容的分析与界定是科学的，符合目前我国信息安全学科的实际情况。

（3）《规范》的制订工作遵循了“统一与特色相结合，宽口径，最小集合，最低标准，分类指导”的原则，给出了两套信息安全专业的知识体系和实践能力体系的具体方案，供各学校自主选用、自主更换。这一原则符合教育部对规范制定的要求。《规范》所设计的信息安全专业知识体系和实践能力体系是科学的、合理的，符合信息安全学科的自身规律和我国当前信息安全专业发展的实际情况，具有实用性和可操作性。

(4)《规范》描述了信息安全专业培养目标和培养规格,这些描述符合信息安全专业本科人才培养的教育规律,有利于我国信息安全专业的人才培养。

评审专家一致认为,本项目组圆满完成了教育部下达的制定规范的任务,同意通过评审。

评审专家组建议,在设立信息安全专业的学校更广泛地开展《规范》的试用工作,并在此基础上对《规范》作进一步修改,以使《规范》不断完善。

评审专家组组长:沈昌祥

中国工程院院士

2012年11月2日

前言

FOREWORD

指导性专业规范是国家教学质量标准的一种表现形式。指导性专业规范是国家对本科教学质量的最低要求，主要规定本科学生应该学习的基本理论、基本技术和基本应用。不同层次的学校在这个最低要求基础上增加本学校的要求，制订本学校的教学质量标准，体现本学校的办学定位和办学特色。

2006年教育部给武汉大学下达了“信息安全专业指导性专业规范研制”的教学科研项目。2007年“教育部高等学校信息安全类专业教学指导委员会”成立。这个教学科研项目转交给教指委组织实施。在教指委的指导下，项目组团结一致，努力工作，克服困难，历时5年，制定出我国第一个“信息安全专业指导性专业规范”。

《高等学校信息安全专业指导性专业规范》(以下简称为《规范》)已于2012年底通过经教育部高等教育司理工科教育处授权组织的专家组评审，并且已经得到武汉大学等许多高校的实际应用。

实际应用的情况表明，《规范》对信息安全学科的内涵、理论基础、方法论基础、主要研究方向和研究内容的分析与界定是科学的，符合目前我国信息安全学科的实际情况。《规范》所设计的信息安全专业知识体系和实践能力体系是科学的、合理的，符合信息安全学科的自身规律和我国当前信息安全专业发展的实际情况，具有实用性和可操作性。《规范》描述了信息安全专业培养目标和培养规格，这些描述符合信息安全专业本科人才培养的教育规律，有利于我国信息安全专业的人才培养。

在《高等学校信息安全专业指导性专业规范》的制定过程中，教育部高等教育司理工科教育处自始至终给予了具体的指导和帮助。

2013年，新一届“教育部高等学校信息安全专业教学指导委员会”成立。经组织审查和研究决定，2014年以“教育部高等学校信息安全专业教学指导委员会”的名义正式发布《高等学校信息安全专业指导性专业规范》。教指委相信，《规范》的正式出版发行，必将对提高我国信息安全专业建设和人才培养的质量发挥重要作用。

教育部高等学校信息安全专业教学指导委员会

2014年3月

引言

2006 年，教育部给武汉大学下达了“信息安全专业指导性专业规范研制”和“信息安全专业专业评估研究与实践”两个“高等理工教育教学改革与实践项目”。

2007 年，“教育部高等学校信息安全类专业教学指导委员会”(以下简称为“教指委”)成立。这两个教学科研项目转交给“教指委”组织实施。为此，“教指委”专门组织成立了两个项目组开展项目研究。“信息安全专业专业评估研究与实践”项目组由“教指委”主任沈昌祥院士任组长。“信息安全专业指导性专业规范研制”项目组由“教指委”副主任、武汉大学张焕国教授任组长，项目组由 11 位专家组成，他们是武汉大学张焕国教授、山东大学王小云教授、北京电子科技学院方勇教授、北京邮电大学杨义先教授、解放军信息工程大学王清贤教授、北京航空航天大学刘建伟教授、哈尔滨工业大学张宏莉教授、中国刑事警察学院秦玉海教授、电子科技大学秦志光教授、上海交通大学来学嘉教授、清华大学出版社张民副编审。为了使项目组更具广泛的代表性，项目组聘请了南开大学的贾春福教授和西安电子科技大学的李晖教授作为特邀专家参加项目组的工作。

2007 年 4 月，项目组在清华大学出版社召开了第一次全体会议，宣布制定信息安全专业规范的研究工作正式启动，并讨论了具体的工作计划和任务分工。会议之后的第一件工作是设计制定了“信息安全本科毕业生现状及人才需求调查问卷”，并在全国范围开展了大规模的问卷调查。先后共发出调查问卷一千多份，回收五百多份。项目组对回收的调查问卷进行了统计分析，为专业规范的制定提供了社会需求的基础数据。同时，项目组又认真学习了计算机科学与技术专业规范和电子信息科学与工程类专业规范，

引言

从中得到了许多有益的启发，为信息安全专业规范制定工作提供了参考和借鉴。

接下来进入了专业规范制定阶段。在项目组专家的指导下，武汉大学计算机学院信息安全系的几乎所有老师都参与了这一工作。

2007 年 11 月，“第一届中国信息安全学科建设与人才培养研讨会”在武汉大学召开，项目组向会议做了规范制定的报告，并向会议提交了《信息安全专业规范（第一次征求意见稿）》。会后，根据与会代表的意见和建议，项目组又进行了修改。在这之后，项目组又在清华大学出版社先后召开了两次全体会议，讨论修改规范草稿。2008 年 10 月，“第二届中国信息安全学科建设与人才培养研讨会”在电子科技大学召开，项目组向会议提交了《信息安全专业规范（第二次征求意见稿）》。这是专业规范第二次在全国范围内进行广泛征求意见。2009 年 3 月底，在北京香山饭店召开了“教育部高等学校信息安全类专业教学指导委员会 2009 年度工作会议”。项目组向会议做了《规范》制定工作的汇报。委员们对《规范》展开了热烈讨论，充分发表了意见。2009 年 8 月，“第三届中国信息安全学科建设与人才培养研讨会”在中国刑事警察学院召开，项目组又向会议提交了《信息安全专业规范（第三次征求意见稿）》，第三次在全国范围内进行广泛征求意见。2010 年 3 月 17 日，在北京西郊宾馆召开了“教育部高等学校信息安全类专业教学指导委员会 2010 年度工作会议”。项目组又一次向会议做了规范制定工作的汇报。委员们建议将“信息内容安全”明确提升为一个独立的知识领域。会后，项目组根据“教指委”会议的意见对《规范》进行了进一步的修订，形成了最后的提交版本。

引言

2010年5月，项目组决定将此版本提交给教育部高教司进行评审。

2012年11月2日，“第六届中国信息安全学科建设与人才培养研讨会”在天津理工大学召开。经教育部高教司理工处批准，在天津理工大学召开了《高等学校信息安全专业指导性专业规范》评审会。评审会对《高等学校信息安全专业指导性专业规范》及项目组的工作给予了高度评价，并建议作进一步修改后正式出版发行并广泛开展试用工作。

在天津评审会议之后，为了《规范》的出版，项目组又对《规范》进行了一次彻底的检查修订。首先是检查修正了《规范》中的一些文字和语句问题，同时也少量调整了《规范》中的一些技术内容，例如增加了“隐私保护”方面的内容。

本《规范》制定的一个特点是，在《规范》基本形成之后，便开始了《规范》的实际应用。武汉大学作为《规范》制定的牵头单位，率先进行了《规范》的全面应用，还有许多其他学校也进行了《规范》的部分实际应用。这些对《规范》的应用实践给我们反馈了许多修改《规范》的意见和建议，使我们能够把《规范》制定得更好。另一方面，这些对《规范》的实际应用也表明了我们所制定的《规范》的可用性。现在，在《规范》正式出版之际，我们把武汉大学信息安全专业贯彻执行《规范》的一些教学文件作为附录，供其他学校参考。

我们走过了5年多的《规范》制定历程，项目组深深地体会到：制定我国信息安全专业指导性专业规范是我国教育史上的第一次，具有重要的意义。但是，由于信息安全是一个新兴学科，在我国开办信息安全专业的时间还不长，我们缺乏制定专业规范的经验，而且信息安全科学技术发展太快，从而使得规范的制定成为一件极其困难、极其艰巨的工作。

引言

FOREWORD

在"教指委"的指导下,项目组团结一致,努力工作,克服困难,胜利地完成了任务,制定出我国第一个《高等学校信息安全专业指导性专业规范》。

项目组深知,目前的规范仍然有一些不尽满意的地方。随着信息安全科学技术的发展和信息安全专业规范的实际应用,应当继续对《规范》进行修订和完善。项目组相信,经过信息安全专业规范的实际应用和进一步修订后,我们的专业规范一定可以成为一个适应我国信息安全专业建设和人才培养需要的、有特色的专业规范。

"信息安全专业指导性专业规范研制"项目组组长:张焕国

2013 年 7 月 18 日

目录

CONTENTS

CONTENTS

目录

目录

CONTENTS

第1章 信息安全学科

21 世纪是信息科学与技术飞速发展的时代。信息成为一种重要的战略资源。信息的获取、存储、处理及其安全保障能力成为一个国家综合国力的重要组成部分。目前，信息产业已成为世界第一大产业，信息科学与技术正处于空前繁荣的阶段。信息安全是信息的影子，哪里有信息，哪里就有信息安全问题。在信息科学与技术空前繁荣的同时，危害信息安全的事件不断发生，信息安全的形势是严峻的。信息安全事关国家安全、事关社会稳定，必须采取措施确保我国的信息安全。

2004 年，党的十六大文件已经把信息安全作为我国国家安全的重要组成部分。2009 年，国家主席胡锦涛在第 64 届联合国大会一般性辩论会上强调了信息安全等非传统安全的重要性。2012 年，党的十八大文件进一步明确指出要“高度关注海洋、太空、网络空间安全”。因此，加快国家信息安全保障体系建设，确保我国的信息安全，已经成为我国的国家战略。

人才资源是第一位的资源。因此，信息安全人才培养是我国国家信息安全保障体系建设的必备基础和先决条件。信息安全学科建设则是建设培养高层次信息安全专业人才的基础平台。

1.1 信息安全学科的内涵

目前业界关于信息安全学科的定义和内涵，尚未形成一个统一的说法。不同的学者根据自己的研究和理解，给出了不同的诠释。尽管这些诠释不尽相同，但是其主要内容却是相同的。

传统的信息安全强调信息（数据）本身的安全属性，认为信息安全主要包含以下几个方面：

① **信息的秘密性**：使信息不泄露给未授权者的特性。

② **信息的完整性**：保护信息真实、完整和未被修改的特性。

③ **信息的可用性**：已授权实体一旦需要就可访问和使用信息的特性。

信息论的基本知识告诉我们，信息不能脱离它的载体而孤立存在，因此我们不能脱离信息系统而孤立地谈论信息安全。这也就是说，每当我们谈论信息安全时总是不可避免地要谈论信息系统的安全。这是因为，如果信息系统的安全受到危害，则必然会危害到存在于信息系统之中的信息的安全。据此，我们应当从信息系统角度来全面考虑信息安全的内涵。

从纵向来看，信息系统安全主要包括以下 4 个层面：设备安全，数据安全，内容安全，行为安全。其中，数据安全即是传统的信息安全。

（1）**设备安全**：信息系统设备（硬设备和软设备）的安全是信息系统安全的首要问题。这里包括三个侧面：

① 设备的稳定性；

② 设备的可靠性；

③ 设备的可用性。

（2）**数据安全**：采取措施确保数据免受未授权的泄漏、篡改和毁坏。

① 数据的秘密性；

② 数据的完整性；

③ 数据的可用性。

（3）**内容安全**：内容安全是信息安全在政治、法律、道德层次上的要求。

① 信息内容在政治上是健康的；

② 信息内容符合国家法律法规；

③ 信息内容符合中华民族优良的道德规范。

（4）**行为安全**：行为安全从主体行为的过程和结果来考察是否会危害

信息安全，或者，是否能够确保信息安全。从行为安全的角度来分析和确保信息安全，符合哲学上实践是检验真理唯一标准的基本原理。

① 行为的秘密性：行为的过程和结果不能危害数据的秘密性，必要时行为的过程和结果也应是保密的；

② 行为的完整性：行为的过程和结果不能危害数据的完整性，行为的过程和结果是预期的；

③ 行为的可控性：当行为的过程出现偏离预期时，能够发现、控制或纠正。

根据上面的分析，要确保信息系统的安全，就必须确保信息系统的设备安全、数据安全、内容安全和行为安全。信息系统的硬件系统安全和操作系统安全是信息系统安全的基础，密码和网络安全等技术是信息系统安全的关键技术。确保信息系统安全是一个系统工程，只有从信息系统的硬件和软件的底层做起，从整体上采取措施，才能比较有效地确保信息系统的安全。

为了表述简单，在不会产生歧义时可以直接将信息系统安全简称为信息安全。实际上，在多数情况下是不会产生歧义的，而且大家已经这样称呼了。

综上所述，我们给出信息安全学科的内涵：**信息安全学科是研究信息获取、信息存储、信息传输和信息处理中的信息安全保障问题的一门新兴学科**。

信息安全学科是综合计算机、通信、电子、数学、物理、生物、管理、法律和教育等学科，并发展演绎而形成的交叉学科。信息安全学科与这些学科既有紧密的联系和渊源，又具有本质的不同，从而构成了一个独立的学科。信息安全学科是研究信息的获取、存储、传输和处理中的安全保障问题的一门新兴学科。信息安全学科已经形成了自己的理论、技术和应用，并服务于信息社会。

信息安全学科归属于工学，但考虑到现阶段我国的信息安全专业的实

际情况，允许学校给信息安全专业的毕业生授予工学、理学或管理学学士学位。

1.2 国外信息安全学科的状况

美国等发达国家十分重视信息安全，把确保信息系统安全作为国家安全战略中最重要的组成部分之一。多年来，美国一直把网络空间安全作为其国防安全的重点，多层次培养信息安全人才，大力发展信息安全技术，并且形成了庞大的信息安全产业，走在世界各国的前头。

美国历届政府都高度重视信息安全，制定和颁布了一系列的规划和计划，并加以实施。早在1995年，美国国家安全局（National Security Agency）就委托卡耐基梅隆大学成立了信息安全学术人才中心，以提高大学信息安全人才培养能力。至2003年9月，已有五十多所教育机构被认定成为这种中心，其中一部分大学设立了信息安全本科专业，一部分大学设立了信息安全硕士专业，更多的大学校设立了信息安全研究方向。

除此之外，美国的麻省理工学院、卡耐基梅隆大学、加州大学伯克利分校、斯坦福大学等名牌大学长期与美国军方合作，不仅为军方完成了许多重要的研究项目，还为军方培养了大批高层次信息安全专业人才。

2009年5月29日，奥巴马政府公布了名为《信息空间政策评估——保障可信和强健的信息和通信基础设施》的报告。其中，把信息安全教育和人才培养列为重点之一。正式提出了信息安全劳动力的概念，从而把信息安全作为一种新的社会职业。

2010年4月，美国政府启动了“网络空间安全教育国家计划”（National Initiative for Cybersecurity Education，NICE）。该计划由美国商务部NIST研究所牵头，国土安全部、国防部、教育部、司法部等11个政府部门共同负责。NICE计划的目的是通过创新网络空间安全教育，增强美国整体的网络空间安全，并制定了三个具体目标：

（1）提高全民网络空间安全的风险意识；

（2）扩充网络空间安全队伍后备人才；

（3）培养一支具有全球竞争力的网络空间安全队伍。

为了实施 NICE 计划，NICE-NIST 委员会专门制定了相关的指导文件。2011 年 8 月发布了《NICE 战略计划（草案）》并在网上公开征集意见。2012 年 9 月又发布了修改草案。草案将网络空间安全技术领域分为 7 个大类：

（1）安全地提供保障；

（2）系统运行与维护；

（3）实施保护与防御；

（4）调查取证；

（5）情报收集与作战；

（6）事态与信息分析；

（7）监管与发展。

NICE 计划的启动和系统细致地组织实施充分表达了美国对信息安全问题的深刻认识和高度重视，这些值得我们借鉴。

1.3　我国信息安全学科的发展历程

我国在信息安全领域的工作和技术，早在红军时期就开始了，我党我军的密码工作已经经历了八十多年的发展历程。在革命战争年代，人民军队在密码技术方面的成功，为赢得战争胜利和新中国的建立作出了杰出的贡献。老一代中国密码人的杰出功勋，将永远铭记在中国人民的心中。

我国在信息安全领域的工作和技术已经经历了通信保密、信息安全和信息安全保障三个阶段。

通信保密阶段：在计算机开始广泛应用之前，我国在信息安全领域的工作和技术主要是确保通信的保密，所使用的信息安全技术主要是密码技

术。只有少数专业单位进行密码技术的研究和开发，而且研究开发工作本身也是秘密进行的。1982 年，西安电子科技大学邀请日本京都大学一松信教授来华讲学："计算复杂性与密码学"；1984 年 12 月，在西安电子科技大学召开了"第一届中国密码学术会议"。这些活动开创了我国民间公开研究密码学的先河。

信息安全阶段：20 世纪 80 年代中期以后，微机的应用逐渐广泛。计算机病毒开始出现并广泛传播，非法拷贝软件的现象也相当普遍。随着网络技术的发展和应用，计算机病毒、蠕虫和木马等恶意代码通过网络传播，造成了更大范围的危害。于是，防治计算机病毒等恶意代码，阻止非法拷贝软件，保障网络安全成为社会对信息安全的迫切需要。这一时期，除了通信保密之外，计算机操作系统安全、分布式系统安全和网络系统安全的重要性和紧迫性逐渐突现出来。为了解决这些信息安全问题，出现了计算机安全、软件保护、网络安全等信息安全新内容和新技术。

信息安全保障阶段：进入 21 世纪，通信、计算机和消费电子(Communication，Computer，Consumer electronics) 的结合，促进了因特网、信息高速公路或全球信息基础设施(GII)的出现和应用，构成了人类生存的信息环境，即信息空间(Cyberspace)。

人们清楚地认识到，人类社会中的安全可信与信息空间中的安全可信是休戚相关的。对于人类生存来说，只有同时解决人类社会和信息空间的安全可信，才能保证人类社会的安全、和谐、繁荣和进步。

在信息空间时代，信息科学技术和产业空前繁荣，社会的信息化程度大大提高。电子商务和电子政务等大型应用信息系统开始广泛应用，云计算、物联网、大数据处理等新型信息系统出现。这些都对信息安全提出了更新更高的要求。信息成为一种重要的战略资源，任何危害信息安全的行为都将可能造成重大损失。这时，对信息安全的要求不仅是单纯的通信保密和传统意义上的信息安全，已经上升到信息系统安全的阶段（设备安全、数据安全、内容安全、行为安全）。人们对信息安全内涵和属性的理

解也有了很大的扩展，可信性、隐私性、强健性和可生存性等成为信息系统安全的新属性。可信计算等信息系统安全新技术出现，确保信息空间的安全可信成为新的目标。我国在信息安全领域的工作和技术进入信息安全保障阶段。

在 20 世纪 70 年代之前，我国只有少数专业性学校（如军队学校）培养信息安全方面的专业人才，而且培养的技术内容以密码技术为主。从 20 世纪 70 年代开始，我国普通高校开始培训信息安全人才。例如，中国科学院数学研究所和北京大学开始为军队培训密码学的数学基础，西安电子科技大学开始为军队培训数字通信和编码。此后，在高校恢复研究生制度以后，西安电子科技大学等少数高校开始招收密码学的研究生。

1999 年，西安电子科技大学等 4 所高校建立了“信息对抗”本科专业。

2001 年，武汉大学建立了我国第一个信息安全本科专业，我国从此开始培养信息安全本科人才。同年，武汉大学与企业合作又建立了我国第一个“信息安全博士后产业基地”。到目前为止，全国已经有八十多所高校建立了信息安全本科专业。2003 年，武汉大学、华中科技大学、中国科学院软件所和国防科技大学率先建立了信息安全博士点。后来，建立信息安全博士点的高校又增加了很多。除了信息安全博士点外，西安电子科技大学、解放军信息工程大学、北京邮电大学和国防科技大学等高校还建立了密码学博士点。从此，我国形成了从本科到博士后的完整的信息安全人才培养体系。2005 年，教育部下达了《教育部关于进一步加强信息安全学科、专业和人才培养工作的意见》的文件。文件提出，“不断加强信息安全学科、专业建设，尽快培养高素质的信息安全人才队伍，成为我国经济社会发展和信息安全体系建设中的一项长期性、全局性和战略性的任务”。2006 年，教育部给武汉大学下达了“信息安全专业指导性专业规范研制”和“信息安全专业专业评估研究与实践”两个教学科研项目。2007 年 1 月，“教育部高等学校信息安全类专业教学指导委员会”成立。同年年底，

教育部批准了15所高校的信息安全专业为“国家特色专业建设点”。2012年，我国政府发布了《国务院关于大力推进信息化发展和切实保障信息安全的若干意见》的文件，文件进一步强调了“支持信息安全与保密学科师资队伍、专业院系、重点实验室建设”。

从此我国信息安全学科、专业建设与人才培养工作进入了规范化、高质量的发展阶段。

发展我国的信息安全事业，人才培养是关键。教育是人才培养的基础，高校是人才培养的基地。普遍提高我国高校学生的信息安全意识，提高他们对信息安全风险的认识和基本防护能力，已经成为我国每一所高校必须高度重视的教育问题。其中，如何有效地培养出适应社会需求的、多层次高素质的信息安全专业人才，已经成为我国设置信息安全专业高校的一项重要任务。

1.4 信息安全学科的主要研究方向及研究内容

当前，信息安全学科的主要研究方向有密码学、网络安全、信息系统安全，信息内容安全和信息对抗。可以预计，随着信息安全科学技术的发展和应用，一定还会产生新的信息安全研究方向，信息安全的研究内容将更加丰富。

下面分别介绍这5个研究方向的研究内容。

1.4.1 密码学

密码学由密码编码学和密码分析学组成，其中，密码编码学主要研究对信息进行编码以实现信息隐蔽，而密码分析学主要研究通过密文获取对应的明文信息。密码学研究密码理论、密码算法、密码协议、密码技术以及密码应用等科学技术问题。其主要研究内容有：

① 对称密码；

② 公钥密码；

③ Hash 函数；

④ 密码协议；

⑤ 新型密码（生物密码，量子密码等）；

⑥ 密钥管理；

⑦ 密码应用。

1.4.2　网络安全

网络安全的基本思想是在网络的各个层次和范围内采取防护措施，以便能够对各种网络安全威胁进行检测发现，并采取相应的响应措施，确保网络的信息安全。其中，防护、检测和响应都需要基于一定的安全策略和安全机制。网络安全的研究包括网络安全威胁、网络安全理论、网络安全技术和网络安全应用等。其主要研究内容有：

① 网络安全威胁；

② 通信安全；

③ 协议安全；

④ 网络防护；

⑤ 入侵检测；

⑥ 入侵响应；

⑦ 可信网络。

1.4.3　信息系统安全

信息系统是为用户提供服务的各种软硬件系统，用户通过信息系统得到信息的服务。有的信息系统较小，但许多信息系统是复杂庞大的系统，如操作系统、数据库系统、电子商务系统、电子政务系统等都是复杂庞大的典型信息系统。

信息系统是信息的载体，信息系统应当确保存在于其中的信息的安

全。信息系统安全的特点是从系统的整体上考虑信息安全威胁并采取防护措施。它研究信息系统的安全威胁、信息系统安全的理论、信息系统安全技术和应用，其主要研究内容有：

① 信息系统的安全威胁；

② 信息系统的设备安全；

③ 信息系统的硬件系统安全；

④ 信息系统的软件系统安全；

⑤ 访问控制；

⑥ 可信计算；

⑦ 信息安全等级保护；

⑧ 信息系统安全测评认证；

⑨ 应用信息系统安全。

1.4.4 信息内容安全

信息内容安全是信息安全在政治、法律、道德层次上的要求。我们要求信息内容是安全的，就是要求信息内容在政治上是健康的，在法律上是符合国家法律法规的，在道德上是符合中华民族优良的道德规范的。

1995年，西方七国信息会议首次提出“数字内容产业”（Digital Content Industry)的概念。我国将“数字内容产业”定义为基于数字化、网络化，利用信息资源创意、制作、开发、分销、交易的产品和服务的产业。显然，数字内容产业需要信息内容安全来保障。若不能确保信息内容的安全，将不能确保数字内容产业的健康发展。

目前学术界对信息内容安全的认识尚不一致。广义的信息内容安全既包括信息内容在政治、法律和道德方面的要求，也包括信息内容的保密、知识产权保护、隐私保护等诸多方面。这里主要强调信息内容安全中的基本概念、基本理论、基本技术和应用。其主要研究内容有：

① 信息内容安全的威胁；

② 信息内容的获取；

③ 信息内容的分析与识别；

④ 信息内容的管控；

⑤ 信息隐藏；

⑥ 隐私保护；

⑦ 信息内容安全管理；

⑧ 信息内容安全的法律保障。

1.4.5 信息对抗

随着计算机网络的迅速发展和广泛应用，信息领域的对抗从电子对抗发展到信息对抗。

信息对抗就是为削弱、破坏对方电子信息设备和信息的使用效能，保障己方电子信息设备和信息正常发挥效能而采取的综合技术措施，其实质是斗争双方利用电磁波和信息的作用来争夺电磁频谱和信息的有效使用和控制权。

信息对抗研究信息对抗的理论、信息对抗技术和应用。其主要的研究内容有：

① 通信对抗；

② 雷达对抗；

③ 光电对抗；

④ 计算机网络对抗。

1.5 信息安全学科的理论基础和方法论基础

信息安全学科是在计算机、通信、电子、数学、物理、生物、法律、管理和教育等学科的基础上交叉融合发展而来的，其理论基础和方法论基础也与这些学科相关，但在学科的形成和发展过程中又丰富和发展了这些

理论和方法论，从而形成了自己的学科理论和方法论。

1.5.1 理论基础

1. 数学

数学是一切自然科学的理论基础，当然也是信息安全学科的理论基础。

现代密码可以分为两类：一类是基于数学的密码，另一类是基于非数学的密码。虽然某些基于非数学的密码技术开始走向应用，例如基于量子物理的量子密钥分发技术。但是，基于非数学的密码总体上还处在发展的初期阶段。目前广泛实际应用的密码仍然主要是基于数学的密码。

对于基于数学的密码，本质上一个密码就是一个数学函数，而密码破译就是求解某一数学难题。这就清晰地阐明了数学是密码学的理论基础。作为密码学理论基础之一的数学主要有代数、数论、概率统计等。

协议是网络的核心，因此协议安全是网络安全的核心。作为网络协议安全理论基础之一的数学主要有逻辑学等。

因为信息安全领域的斗争，本质上是对抗双方之间的斗争，因此数学中的博弈论便成为信息安全的基础理论之一。

博弈论（Game Theory）是现代数学的一个分支，是研究具有对抗或竞争性质的行为的理论与方法。一般而言，称具有对抗或竞争性质的行为为博弈行为。在博弈行为中，参加对抗或竞争的各方各自具有不同的目标或利益，并力图选取对自己最有利的或最合理的方案。博弈论研究的就是博弈行为中对抗各方是否存在最合理的行为方案，以及如何找到这个最合理的方案。博弈论考虑对抗双方的预期行为和实际行为，并研究其优化策略。博弈论的思想古已有之，我国古代的《孙子兵法》不仅是一部军事著作，而且是最早的一部博弈论专著。博弈论已经在经济、军事、体育和商业等领域得到广泛应用。信息安全领域的斗争无一不具有这种对抗性或竞争性。例如，网络的攻与防、密码的加密与破译、病毒的制毒与杀毒、信

息内容的隐藏与提取，等等。因为信息安全领域的斗争，本质上都是人与人之间的对抗性质的斗争，因此博弈论便成为信息安全的基础理论之一。遵循博弈论的指导原则，我们将在信息安全的斗争中，避免被动，掌握主动，立于不败之地。

2. 信息论、控制论和系统论

信息论、控制论和系统论是现代科学的理论基础，也是信息安全学科的理论基础。

信息论是商农为解决现代通信问题而建立的；控制论是维纳在解决自动控制问题中建立的；系统论是为了解决现代化大科学工程项目的组织管理问题而建立的。在开始时，它们都是独自形成的独立科学理论。但由于它们之间具有紧密的联系，因此在后来的应用和发展中互相渗透、互相作用，出现了趋向综合统一、形成统一学科的趋势。这些理论，特别是信息论构成了信息安全学科的理论基础。

信息论对信息源、密钥、加密和密码分析进行了数学分析，用不确定性和唯一解距离来度量密码体制的安全性，阐明了密码体制、完善保密、纯密码、理论保密和实际保密等重要概念，把密码置于坚实的数学基础之上，标志着密码学作为一门独立学科的形成。因此，信息论成为密码学的重要的理论基础之一。

从信息论角度看，信息隐藏（嵌入）可以理解为在一个宽带信道(原始宿主信号)上用扩频通信技术传输一个窄带信号（隐藏信息）。尽管隐藏信号具有一定的能量，但分布到信道中任意特征上的能量是难以检测的。隐藏信息的检测是一个有噪信道中弱信号的检测问题。因此，信息论构成了信息隐藏的理论基础。

综上所述，信息论奠定了密码学和信息隐藏的理论基础。虽然密码学和信息隐藏已经取得了重要发展并得到了广泛应用，但是密码学和信息隐藏的发展至今没有超越信息论的理论范畴。

系统论是研究系统的一般模式、结构和规律的科学。系统论的核心思想是整体观念。任何一个系统都是一个有机的整体，不是各个部件的机械组合和简单相加。系统的功能是各部件在孤立状态下所不具有的。系统论的能动性不仅在于认识系统的特点和规律，更重要的是在于利用这些特点和规律去控制、管理、改造或创造一个系统，使它的存在和发展符合人的需求。

控制论是研究机器、生命社会中控制和通信的一般规律的科学。它研究动态系统在变化的环境条件下如何保持平衡状态或稳定状态。控制论中把“控制”定义为，为了改善受控对象的功能或状态，获取一些信息，并以这种信息为基础施加作用到该对象上。由此可见，控制的基础是信息，信息的获取是为了控制，任何控制又都依赖于信息反馈。

信息安全遵从“木桶原理”。这“木桶原理”正是系统论的思想在信息安全领域的体现。

保护、检测、反应（PDR）策略是确保信息系统和网络安全的基本策略。在信息系统和网络系统中，系统的安全状态是系统的平衡状态或稳定状态。恶意软件的入侵打破了这种平衡和稳定。检测到这种入侵，便获得了控制的信息，进而杀灭这些恶意软件，使系统恢复安全状态。

确保信息系统安全是一个系统工程，只有从信息系统的硬件和软件的底层做起，从整体上采取措施，才能比较有效地确保信息系统的安全。

以上策略和观点已经经过信息安全的实践检验，证明是正确的，是行之有效的。它们符合系统论和控制论的基本原理。这表明，系统论和控制论是信息系统安全和网络安全的理论基础。

3. 计算理论

信息安全学科的许多问题是计算安全问题，因此计算理论也是信息安全学科的理论基础，主要包括可计算性理论和计算复杂性理论等。

可计算性理论是研究计算的一般性质的数学理论。它通过建立计算的

数学模型，精确区分哪些问题是可计算的，哪些问题是不可计算的。对于判定问题，可计算性理论研究哪些问题是可判定问题，哪些问题是不可判定问题。

计算复杂性理论使用数学方法对计算中所需的各种资源的耗费作定量的分析，并研究各类问题之间在计算复杂程度上的相互关系和基本性质。计算复杂性理论是计算理论在可计算性理论之后的又一个重要发展。可计算性理论研究区分哪些问题是可计算的，哪些问题是不可计算的，但是这里的可计算是理论上的可计算，或原则上的可计算。而计算复杂性理论则进一步研究现实的可计算性，如研究计算一个问题类需要多少时间，多少存储空间。研究哪些问题是现实可计算的，哪些问题虽然是理论可计算的，但因计算复杂性太大而实际上是无法计算的。

众所周知，授权是信息系统访问控制的核心，信息系统是安全的，其授权系统必须是安全性的。可计算性的理论告诉我们：一般意义上，对于给定的授权系统是否安全这一问题是不可判定问题，但是一些“受限”的授权系统的安全问题又是可判定问题。由此可知，一般操作系统的安全问题是一个不可判定问题，而具体的操作系统的安全问题却是可判定问题。又例如，著名的“停机问题”是不可判定问题，而具体程序的停机问题却是可判定的。由此可知，一般计算机病毒的检测是不可判定问题，而具体软件的计算机病毒检测又是可判定问题。这就说明了可计算性理论是信息系统安全的理论基础之一。

本质上，密码破译就是求解一个数学难题，如果这个难题是理论不可计算的，则这个密码就是理论上安全的。如果这个难题虽然是理论可计算的，但是由于计算复杂性太大而实际上不可计算，则这个密码就是实际安全的，或计算上安全的。“一次一密”密码是理论上安全的密码，其余的密码都只能是计算上安全的密码。根据计算复杂性理论的研究，NPC 问题是最难计算的一类问题。公钥密码的构造往往基于一个 NPC 问题，以使密码是计算上安全的。例如，McEliece 密码基于纠错码的一般译码是 NPC

问题，背包密码基于求解一般背包问题是 NPC 问题，MQ 密码基于多变量二次非线性方程组的求解问题是 NPC 问题，等等。这说明计算复杂性理论是密码学的理论基础之一。

综上可知，数学、信息论、控制论、系统论、可计算性理论、计算复杂性理论等是信息安全学科的理论基础。

1.5.2 方法论基础

笛卡儿在 1637 年出版了著作《方法论》，他研究并论述了解决问题的方法，对西方人的思维方式和科学研究方法产生了极大的影响。笛卡儿在书中把研究的方法划分为 4 步：

① 永不接受任何我自己不清楚的真理。对自己不清楚的东西，不管是什么权威的结论，都可以怀疑。

② 将要研究的复杂问题，尽量分解为多个比较简单的小问题，一个一个地解决。

③ 将这些小问题从简单到复杂排序，先从容易解决的问题入手。

④ 将所有问题解决后，再综合起来检验，看是否完全，是否将问题彻底解决了。

按不同层次，方法论分为哲学方法论、一般科学方法论和具体科学方法论。其中，研究认识世界、改造世界的最一般的方法论是哲学方法论；研究各科学门类，具有一定普遍意义、适用于各科学门类的方法论是一般科学方法论；研究某一具体科学，涉及这一具体科学的方法论是具体科学方法论。三者之间的关系是相互依存，互相影响，互相补充的对立统一的关系。哲学方法论在一定意义上具有决定性作用，是最一般的方法论，对一般科学方法论和具体科学方法论具有指导意义。

笛卡儿的方法论强调了把复杂问题分解成一些细小的问题分别解决，是一种分而治之的思想。但是它忽视了各个部分的关联和彼此影响。近代科学的发展使科学家发现，许多复杂问题无法分解，或分解后的细小问题

的性质之和并不能反映原问题的性质，因此必须用整体的思想和方法来处理，由此导致系统工程的出现。方法论由传统的方法论发展到系统性的方法论。系统工程的出现推动了环境科学、气象学、生物学、人工智能和软件工程的快速发展。

信息安全保障体系是由信息基础设施、安全防御体系、技术规范与标准、法律法规和组织管理等组成。而信息安全保障体系的实施，必须以人为核心。这就成为一个复杂的系统。因此，解决信息安全领域的问题必须遵循一套科学的方法论，否则是不行的。人们在信息安全保障的长期实践中逐渐形成了自己的方法论。

信息安全学科有自己的方法论，既包含分而治之的传统方法论，又包含综合治理的系统工程方法论，而且将这两者有机地融合为一体。信息安全学科的方法论与数学或计算机科学等学科的方法论既有联系又有区别。具体概括为，**理论分析、逆向分析、实验验证、技术实现4个核心内容**，这四者既可以独立运用，也可以相互结合，指导解决信息安全问题，推动信息安全学科发展。在运用信息安全的方法论分析和解决信息安全问题时，特别强调底层性和系统性。即，从信息系统的软硬件底层和系统结构层来分析信息安全问题，从信息系统的软硬件底层和系统结构层综合采取措施来解决信息安全问题。

其中的逆向分析是信息安全学科所特有的方法论。这是因为信息安全领域的斗争，本质上都是攻防双方之间的斗争，信息安全学科的每一分支都具有攻和防两个方面，因此必须从攻和防两个方面进行分析研究。例如，在进行密码设计时要遵从公开设计原则，即假设对手知道密码算法、掌握足够的明密文数据资源、拥有足够的计算资源，在这样的条件下仍要确保密码是安全的。在进行信息系统安全和网络安全设计时，首先要进行安全威胁分析和风险评估。这些做法就是逆向分析方法论的具体应用，并且已被实践证明是正确的和有效的。

在信息安全学科的方法论的实施过程中，还要注意一个特点，就是必

须坚持“以人为核心”。这是因为，信息安全领域的对抗，本质上是人与人之间的对抗，而人是智能的。不考虑人的因素，是不可能有效解决信息安全问题的。例如，当人们用一个杀病毒软件去查杀一个病毒时，表面上是杀病毒软件与病毒软件之间的斗争，但实际上是编杀病毒软件的人在与编病毒软件的人之间的斗争。

因此，我们应当遵循信息安全学科的方法论，强调底层性和系统性，坚持“以人为核心”，运用定性分析与定量分析相结合、注意量变会引发质变、局部治理与综合治理相结合、追求整体效能，解决信息安全中的理论、技术和应用问题。

1.6 社会对信息安全学科的需求情况及就业前景分析

1.6.1 国家对信息安全的需求

21 世纪是信息的时代，信息成为重要的战略资源。信息技术应用到人们生活和工作的各个方面。社会对计算机和网络等信息系统的依赖越来越大。敌对势力的破坏和恶意软件的攻击等，已对计算机和网络等信息系统的安全构成极大的威胁，如果计算机和网络等信息系统的安全受到破坏，不仅会造成巨大的经济损失，甚至会导致社会混乱。信息安全关系到国家安全、社会稳定、经济发展和人民生活的各个方面，必须确保我国的信息安全。要建设国家信息安全保障体系，政府、军队、公安和企事业都需要大量信息安全专业人才。

1. 政府机构对信息安全的需求

我国政府已经在全国范围内建立起电子政务网和电子党务网。这些网络是政府与党组织联系群众、服务社会的关键基础设施。电子政务网和电子党务网上对信息的保密性、完整性和可用性的要求很高。因此，电子政务网和电子党务网的建设、运行和维护都需要一支品德素质好、专业水平

高的信息安全专业人才队伍。

2. 国防建设对信息安全的需求

信息对抗与网络攻防能力已成为重要的国防力量之一。早在 1995 年美国就提出了信息战的概念，在海湾战争期间美军成功地对伊拉克发动了信息战。2009 年 6 月，美军正式成立了网络司令部，正式把网络作战部队作为一个新的军兵种。2011 年 5 月，美国公布了“网络空间国际战略”，7 月又公布了“网络空间作战战略”，提出“陆、海、空、天、网络”5 维一体的美国国家安全概念。2012 年 1 月，美国宣布“将战略重心放在亚太地区”。

党的十八大文件明确指出要“高度关注海洋、太空、网络空间安全”。因此，加快国家信息安全保障体系建设，确保我国的信息安全，已经成为我国的国家战略。因此，我国也应拥有自己的网络安全队伍。这支网络安全专业队伍与广大人民群众互相配合，共同保障我国的网络空间安全，防范可能的入侵和攻击，并依据法律给予必要的反击。这些都需要大量的高素质信息安全专业人才。

3. 维护社会公共安全对信息安全的需求

近年来，各种形式的网络犯罪给世界许多国家都造成了巨大的损失。

美国政府公布的一份国家安全报告认为，21 世纪对美国国家安全威胁最严重的是网络恐怖主义。美国中央情报局成立了一个专门负责研究遏制计算机犯罪的信息技术中心。为了确保我国的社会公共安全，我国相关职能部门应当依据法律严厉打击网络恐怖和网络犯罪活动。

一些不法分子在网上编造和传播谎言，煽动和组织闹事，破坏民族团结和社会安定。一些网站传播低俗黄色的内容，严重危害青少年的身心健康。

利用计算机信息系统进行经济犯罪，获取经济利益已经在世界范围内

成为一种最严重、最普遍的信息犯罪问题。网上银行诈骗、自动取款机诈骗、电信诈骗、QQ 诈骗、窃取银行账号、伪造银行卡等犯罪事件屡见不鲜，给人民群众造成了重大经济损失，严重影响了社会的安定。

我国是一个大国，每年都要举行一些大型的社会活动。随着社会的信息化，这些大型的社会活动都实现了计算机网络化管理。于是，这些大型社会活动的信息系统也就成为不法分子攻击的目标。为了确保社会活动的正常进行，维护社会安定，必须对这些信息系统进行信息安全防护。例如，为了保障北京奥运会期间的信息安全，2008 年 4 月，北京市专门成立了城市信息安全应急响应与处置中心，中心建立了病毒事件、网络攻击事件、网络入侵、网络事故和应急资源保障等 10 个应急小组。应急响应与处置中心建立了安全预警制度和事件登记制度，以应对城市重要信息系统遭受的非法攻击和系统故障。2010 年上海世博会期间，上海市也建立了专门的信息安全应急响应与处置中心。北京奥运会和上海世博会的成功举办，也有网络信息安全专业人才队伍的一份重要贡献。

由此可见，为了打击各种利用计算机信息系统进行的犯罪活动，维护国家统一、民族团结和社会安全，需要组建专门的网络警察队伍和网络安全群众队伍。这里需要大量的、各种层次的信息安全专业人才。

除此之外，社会的公共安全还与每个公民的信息安全意识相关。在信息化社会中，每个人都生活和工作在信息空间中。公共信息安全应当保护，个人隐私也需要保护。为此，每个人都应具有一定的信息安全常识和信息安全事件的应急处理能力。这就需要对公民进行信息安全的普及教育。这方面也需要大量信息安全专业人才。

1.6.2 经济、金融、商务对信息安全的需求

随着计算机网络技术的发展和广泛应用，促进了社会信息化、经济信息化、金融信息化和商务信息化。于是出现了电子经济管理、电子金融和电子商务等新型经济类信息系统。它们分别是运用计算机和网络技术对经

济信息进行科学处理与管理，对金融业务进行处理和进行各种商务活动的信息系统。电子经济管理、电子金融和电子商务的兴起在经济、金融和商务领域引起了一场革命。由于电子经济管理、电子金融和电子商务系统中的信息是国家的经济命脉和金钱，具有高度的重要性和敏感性，于是这些系统就成为不法分子攻击的重要目标。

攻击各种经济、金融和商务类信息系统，获取经济利益已经在世界范围内成为一种最严重、最普遍的信息犯罪问题。在许多西方发达国家，利用计算机信息系统进行经济犯罪的金额已经超过普通经济犯罪。在我国，利用计算机信息系统进行经济犯罪的事件也在迅猛上升。

要确保经济、金融和商务类信息系统的安全，不仅要防范恶意软件和黑客的攻击，确保经济数据的保密性、完整性和可用性，还要确保电子交易的安全，如网上银行、电子支付和电子货币的安全等。因此，各种经济、金融和商务类信息系统的建设、运营和维护，需要大量的信息安全专业人才。

1.6.3 企事业单位对信息安全的需求

随着信息系统技术的发展和广泛应用，企事业单位的信息系统的规模越来越大，功能越来越强，信息系统的安全隐患也随之增多，企事业单位的信息安全问题也日益严重。如果处置不当，将给企事业单位带来巨大的损失。

在确保信息安全的实践中人们认识到，只有在风险评估、需求分析、系统设计、工程实现、安全测评、运行维护、安全管理各个环节都采取安全措施，才能开发出一套良好的信息系统，并确保系统运行和维护中的信息安全。

我国已经颁布了《信息安全等级保护管理办法》，对企事业单位的信息系统实施等级保护，并对企事业单位必须配备的信息安全专业人员数量作出了硬性规定。我国是一个大国，仅此一项就需要大量的信息安全专业

人才。

1.6.4 信息安全产业的发展对信息安全人才的需求

我国的信息安全产业也已经具有相当的规模，在社会需求和技术进步的推动下，信息安全企业得到迅速的发展。我国是世界上第一人口大国和第二经济总量大国。信息安全市场的需求是巨大的，但是，由于缺乏高级信息安全管理与技术人才和核心技术，因此我国的信息安全产业整体上还比较落后，产业缺乏核心竞争力。这说明我国信息安全企业的发展空间还很大。众多的信息安全企业正在兴起，信息安全服务正在成为一门新兴产业。信息安全产业的发展需要大量信息安全专业人才。

美国已经把信息安全作为一种新的职业，并把信息安全人才作为一种新型劳动力。我国也应当这样做，并应当做得更好。

信息产业已经成为世界第一大产业。信息产业的一个显著特点是发展速度快，每年都会涌现出一些新的技术和新方向。例如，云计算、物联网、三网融合、大数据处理等就是当前涌现出来的新技术和新方向。信息安全是信息的影子，哪里有信息，哪里就有信息安全问题。因此，这些新技术和新方向又给信息安全提出了新的需求。这些信息安全新需求的解决需要大量高层次的信息安全专业人才。

1.6.5 我国信息安全专业毕业生就业前景分析

根据我们的调查分析，目前我国社会对信息安全专业人才的需求大体可分为如下三类。

第一类是理论研究人才。这种需求主要来自于信息安全的专业机构、科研院所、高等院校、大型企业中的信息安全研发机构。用人单位希望这一类人才要掌握信息安全学科某一方向（密码学，网络安全，信息系统安全，信息内容安全）的坚实宽广的基础理论和系统深入的专门知识，具有独立从事科学研究和关键技术开发的能力，通过工作实践能够在科学研究

和关键技术开发方面作出创新性的成果。

第二类是技术开发人才。这种需求主要来自于提供信息安全产品、信息安全服务的各种单位。这方面的人才要具备良好的信息安全基础知识、较强的技术开发能力、通过工作锻炼能够出色完成信息安全产品或服务的设计和开发任务。

第三类是信息安全管理与服务人才。这种需求主要来自于广大企事业单位和政府部门。这方面的人才不仅需要具备较高的信息安全技术能力，能够正确使用、配置、维护信息安全设备，还必须具有一定的法律知识和管理能力，能正确规划、实施和维护信息系统的安全。

在这三类信息安全专业人才中，市场对第一类人才的需求量相对较少，而对第二和第三类信息安全专业人才的需求量极大。

教育部在阳光高考平台上公布了2008年全国本专科专业就业状况，2008年信息安全本科专业就业率为B－（≥80％），其中211高校为B＋（≥85％）。据盈速教育预测的学科专业未来就业指数，“计算机网络安全”学科的就业指数一直保持在88％，比电子、通信与自动控制技术的平均指数78％和计算机科学技术的平均指数65％都要高。

武汉大学自2001年开始招收全国第一届信息安全本科生，目前已经培养了9届毕业生。学生就业率一直保持在90％以上。毕业生的主要就业去向是政府、金融、公安、商务及企事业单位。经过毕业生情况调查，用人单位反映良好。这些都表明，当前我国信息安全专业毕业生的就业情况是良好的。

第2章　高等学校信息安全专业指导性专业规范的构成与制定原则

2.1　高等学校信息安全专业指导性专业规范的构成

根据教育部高教司理工科教育处《高等学校理工科本科指导性专业规范研制要求》，信息安全专业指导性专业规范由以下内容构成：

（1）本专业的学科基础；

（2）本专业的培养目标；

（3）本专业的培养规格；

（4）本专业的知识体系；

（5）本专业的实践能力体系；

（6）本专业的课程体系；

（7）本专业的实践教学体系。

满足社会对信息安全专业毕业生的要求是制定专业规范的最基本的出发点。信息安全学科的基本理论和基本技术，信息安全专业的培养目标和信息安全专业的培养规格是制定信息安全专业规范的基础。

信息安全学科的基本理论和基本技术决定着本规范的知识体系与实践能力体系的内容。毕业生规格是根据社会对信息安全专业毕业生的要求而设定的毕业生应当具备的基本特征。知识体系是毕业生应当具备的知识的结构与集合。知识体系通过课程体系来覆盖、通过教学体系传授给学生。实践能力体系是毕业生应当具备的实践能力的结构与集合。实践能力体系通过实践教学体系来覆盖，通过实践教学体系的实施来培养。而学生的品德素质要在各种教育活动中施教、锻炼、养成。

2.2 制定高等学校信息安全专业指导性专业规范的原则

指导性专业规范是国家教学质量标准的一种表现形式。指导性专业规范是国家对本科教学**质量的最低要求**，主要规定本科学生应该学习的基本理论、基本技术和基本应用。不同层次的学校在这个最低要求基础上增加本学校的要求，制定本学校的教学质量标准，体现本学校的办学定位和办学特色。

根据教育部高教司理工科教育处《高等学校理工科本科指导性专业规范研制要求》和全国信息安全专业的实际情况，我们确定制定高等学校信息安全专业指导性专业规范应当遵循的原则是：**统一与特色相结合，宽口径，最小集合，最低标准，分类指导**。具体阐述如下：

（1）要遵循**统一与特色相结合**的原则。统一本专业的基本要求，给学校留出自己的特色空间。各学校可以在这个基本要求的基础上扩展和增加自己的一些内容与要求，办出自己的特色和优势。这样就既统一了各学校的基本要求，确保了基本办学质量，又体现了各学校的办学特色和优势。从而避免了出现各学校千篇一律的枯燥死板局面，而呈现出百花齐放、万紫千红的繁荣局面。

（2）要遵循**宽口径**的原则。考虑到我国信息安全专业建立的时间不长，主管部门对信息安全学科的认识与管理体制尚未理顺的实际情况，同时考虑到使毕业生容易就业等因素，决定采用宽口径的原则。所谓宽口径，就是规范的知识体系和实践能力体系的覆盖范围比较宽，以使毕业生能够在比较宽的范围内适应用人单位的需求。

（3）要遵循内容**最小集合**的原则。规范中所规定的学习内容是信息安全专业学生所应学习的最小集合。给学生自主学习留出空间，给高校办出自己的特色留出空间。

（4）要遵循核心内容**最低标准**的原则。对于最小集合中的内容，在深

浅程度上取最低标准。

（5）要遵循**分类指导**的原则。为了适应我国八十多所设置信息安全专业的高校在学校类型、办学条件、依托学科和服务面向等方面的不同情况，本专业规范遵循分类指导的原则，制定出一个规范，提供两套方案，供各学校自主选择。

① 第一套方案：培养学生以从事信息安全领域的研究开发工作为主。

② 第二套方案：培养学生以从事信息安全领域的应用服务工作为主。

各高校可以根据自己的实际情况，自主选用，自主调整。例如，一个高校的某一届学生的培养选用了第一套方案，下一届学生的培养也可以选用第二套方案。反之亦然。

第3章　高等学校信息安全专业指导性专业规范

3.1　信息安全专业的学科基础

见本书的第 1 章：信息安全学科。

3.2　信息安全专业的培养目标

信息安全专业培养素质、知识、能力全面发展，具有自然科学、人文科学和信息科学基础知识，掌握信息安全领域的基本理论、基本技术和基本应用，具备信息安全科学研究、技术开发和应用服务工作能力的信息安全专业人才。

3.3　信息安全专业的培养规格

信息安全专业的学制一般为 4 年，合格毕业生授予工学、理学或管理学学士学位。

1. 素质要求

① 思想品德素质：热爱祖国，遵纪守法，具有高度的国家安全意识和信息安全责任心，具有尽职奉献的品德。

② 身心素质：具有良好的身体素质和心理素质。

③ 文化素质：具有一定的文化修养，既要具有一定的中华民族传统优

秀文化的修养，也要具有一定的现代世界文化的修养。

④ 专业素质：具有从事信息安全科学研究、技术开发和应用服务的专业素质，具有一定的创新和创业意识。

2. 知识要求

① 人文社会科学知识：具有文学、外语、法律、管理、艺术等方面的基本知识或常识。

② 自然科学知识：具有与信息安全相关的数学、物理和生物学等方面的基础知识。

③ 专业知识：具有信息安全数学基础、信息科学基础和信息安全基础知识。具有密码学、网络安全、信息系统安全、信息内容安全等领域的专业知识，并在某一方面有所侧重。

3. 能力要求

① 学习能力：具有知识和技术的获取能力，具有自学能力。

② 分析和解决问题的能力：具有信息安全领域的科学研究、技术开发和应用服务的基本能力。

③ 创新能力：具有一定的创新、创业意识和能力。

3.4 信息安全专业规范知识体系

信息安全专业知识体系是信息安全专业毕业生应当具备的知识结构与集合。

知识体系通过课程体系来覆盖，通过教学体系传授给学生。

3.4.1 知识体系的结构

信息安全专业的整体知识体系由自然科学知识体系、人文科学知识体

系和专业知识体系三部分组成。其中，自然科学知识体系和人文科学知识体系是基础，专业知识体系是建立在自然科学知识体系和人文科学知识体系的基础之上的。图 3-1 示出了信息安全专业整体知识体系的结构。

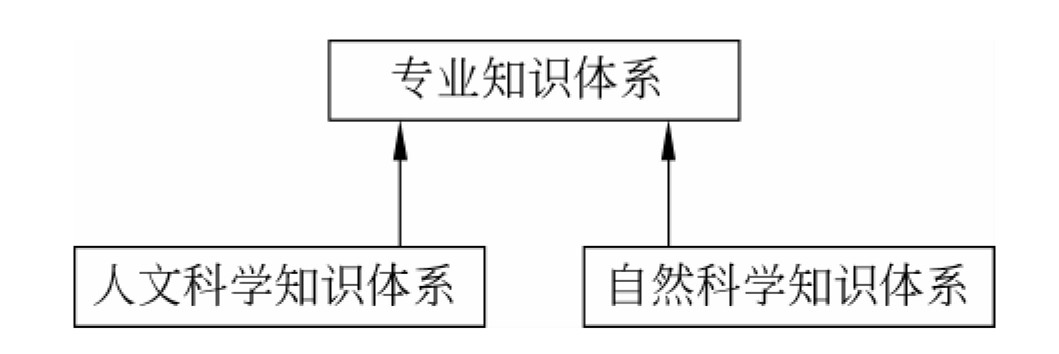


图 3-1　信息安全专业的整体知识体系结构

由于目前各个高校的信息安全专业的依托学科不同，为了给各高校办出自己的特色留出空间，作为基础的自然科学知识体系和人文科学知识体系遵从各学校、学院的整体要求，自主决定。本规范只制定信息安全专业的专业知识体系。

一般情况下，知识体系由知识领域、知识单元和知识点三个层次组成。个别情况下，知识体系由知识领域、子知识领域、知识单元、知识点 4 个层次组成。

一个知识领域或子知识领域由若干个知识单元组成，一个知识单元又由若干个知识点组成。图 3-2 示出了这种层次关系。

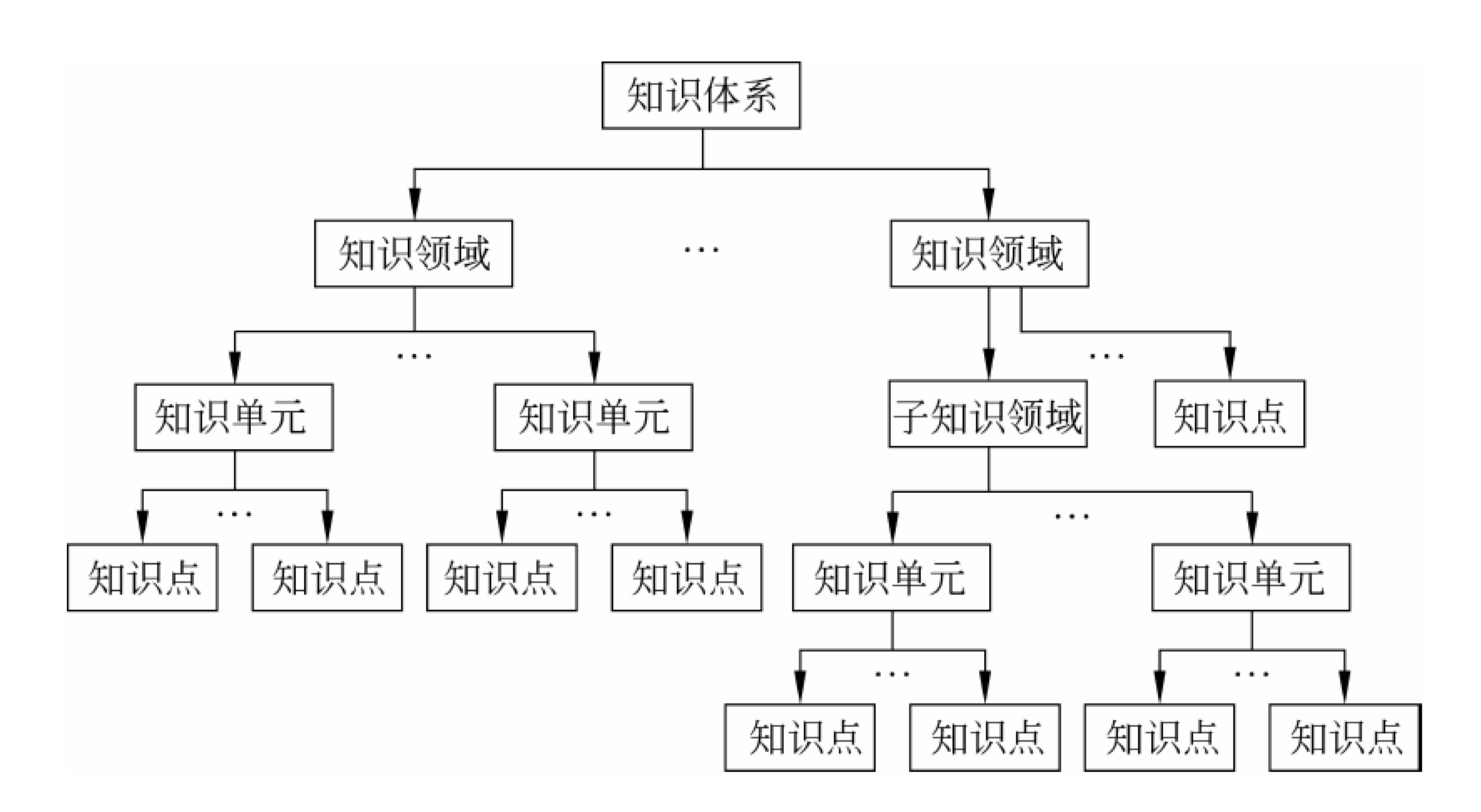


图 3-2　专业知识体系的层次结构

知识单元又分为必修知识单元和选修知识单元。必修知识单元属于信息安全专业学生应当学习的知识的最小集合，是对本专业学生的最基本要求。选修知识单元是指不在必修知识单元内的那些知识单元，选修知识单元供各学校选择学习，以体现自己的办学特色和优势。

本专业规范主要给出信息安全专业的必修知识单元，同时也推荐一些选修知识单元。

图 3-3 示出了信息安全专业的专业知识体系的组成结构。它由信息科学基础知识领域、信息安全基础知识领域、密码学知识领域、网络安全知识领域、信息系统安全知识领域和信息内容安全知识领域组成。

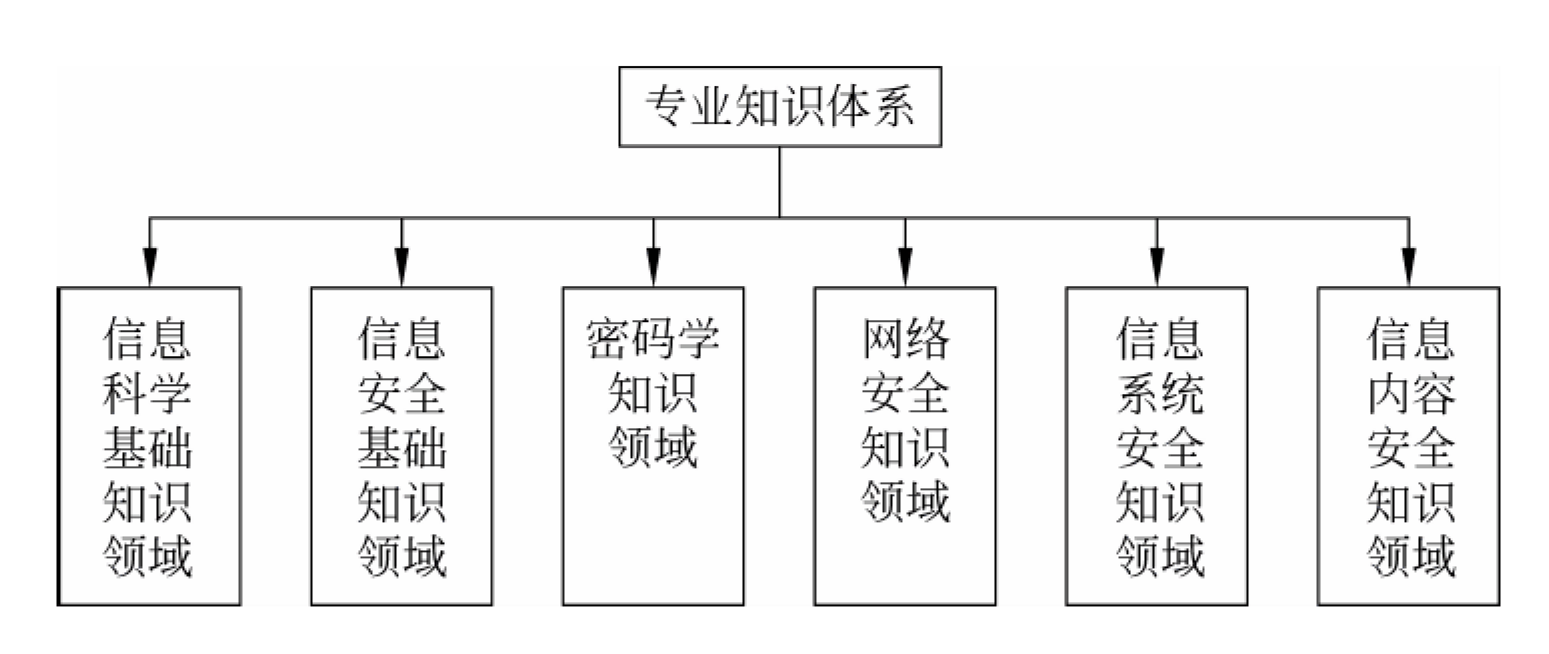


图 3-3　专业知识体系的组成结构

其中的信息科学基础知识领域，由各个学校根据自己的信息安全专业所依托的学科和办学特色自己确定。本规范只制定其余 5 个知识领域的内容。

信息安全界的多数人士普遍认为：目前，信息安全学科的主要研究方向有密码学、网络安全、信息系统安全和信息内容安全。对此，一些学者也有一些不同的认识。本着抓住主要矛盾和求同存异的原则，本专业规范的知识体系暂列出：密码学知识领域，网络安全知识领域，信息系统安全知识领域和信息内容安全知识领域，共 4 个专业知识领域。我们认为，随着信息安全科学技术的发展和应用，不仅会产生一些新的信息安全研究方向，而且老的研究方向也会发生一些变化与融合。到那个时候，专业规范应随之进行调整，以反映信息安全研究方向的新变化。

3.4.2　知识体系中的符号标识

在规范的知识体系中采用了以下符号标识。

① 知识领域用其英文缩写来标识：

- 信息安全基础知识领域（Information Security Base），用 ISB 标识。
- 密码学知识领域，用 CRYPT 标识。
- 网络安全知识领域，用 NS 标识。
- 信息系统安全知识领域，用 ISS 标识。
- 信息内容安全知识领域，用 ICS 标识。

② 知识领域下面的直接知识单元和子知识领域，采用“知识领域标识-序号”的方法来标识。如密码学概念知识单元，用 CRYPT-1 标识。信息安全数学基础子知识领域，用 ISB-2 标识。

③ 子知识领域下面的知识单元，采用“子知识领域标识-序号”的方法来标识。如数论知识单元，用 ISB-2-1 标识。

- 对于知识领域都标示出建议的最少课时数（$x+y$），其中 x 表示建议的最少必修课时数，y 表示建议的最少选修课时数。如 ISB 信息安全基础（52＋82 学时），表明信息安全基础知识领域建议的最少课时数为（52＋82 学时），即建议的最少必修课时数为 52 学时、最少选修课时数为 82 学时。

3.4.3　知识体系方案一

本专业规范遵循分类指导的原则，制定出一个规范，提供两套方案。各高校可以根据自己的实际情况，自主选用，而且在选择之后还可以自主更换。

① 方案一：培养学生以从事信息安全领域的研究开发工作为主。

② 方案二：培养学生以从事信息安全领域的应用服务工作为主。

下面给出知识体系方案一的具体内容。

1. ISB 信息安全基础（52 + 82 学时）

（1）ISB-1 信息安全概念

（2）ISB-2 信息安全数学基础

① ISB-2-1 数论

② ISB-2-2 代数结构

③ ISB-2-3 组合数学（选修）

④ ISB-2-4 逻辑学（选修）

⑤ ISB-2-5 信息论（选修）

⑥ ISB-2-6 编码学（选修）

⑦ ISB-2-7 计算复杂性（选修）

（3）ISB-3 信息安全法律基础

（4）ISB-4 信息安全管理基础

信息安全基础是信息安全学科的一些基础内容。信息安全基础知识领域由信息安全概念知识单元，信息安全数学基础子知识领域、信息安全法律基础知识单元和信息安全管理基础知识单元，共 4 个部分组成。而信息安全数学基础子知识领域又由数论、代数结构、计算复杂性（选修）、逻辑学（选修）、信息论（选修）、编码学（选修）和组合数学（选修），共 7 个知识单元组成。图 3-4 示出了它们之间的结构。

信息安全基础中的信息安全概念主要介绍对信息安全的威胁、信息安全的基本概念和确保信息安全的措施等基本知识。信息安全数学是信息安全学科的理论基础之一，例如，数论、代数结构、组合数学、计算复杂性、信息论等是密码学的理论基础，逻辑学是网络协议安全的理论基础。信息安全法律基础介绍信息安全领域中的一些基本法律知识和我国在信息安全领域的主要法律法规。信息安全管理基础介绍信息安全领域中的一些基本管理知识和方法。信息安全法律和信息安全管理知识则是对整个信息系统安全的设计、实现与应用都有指导性作用的。

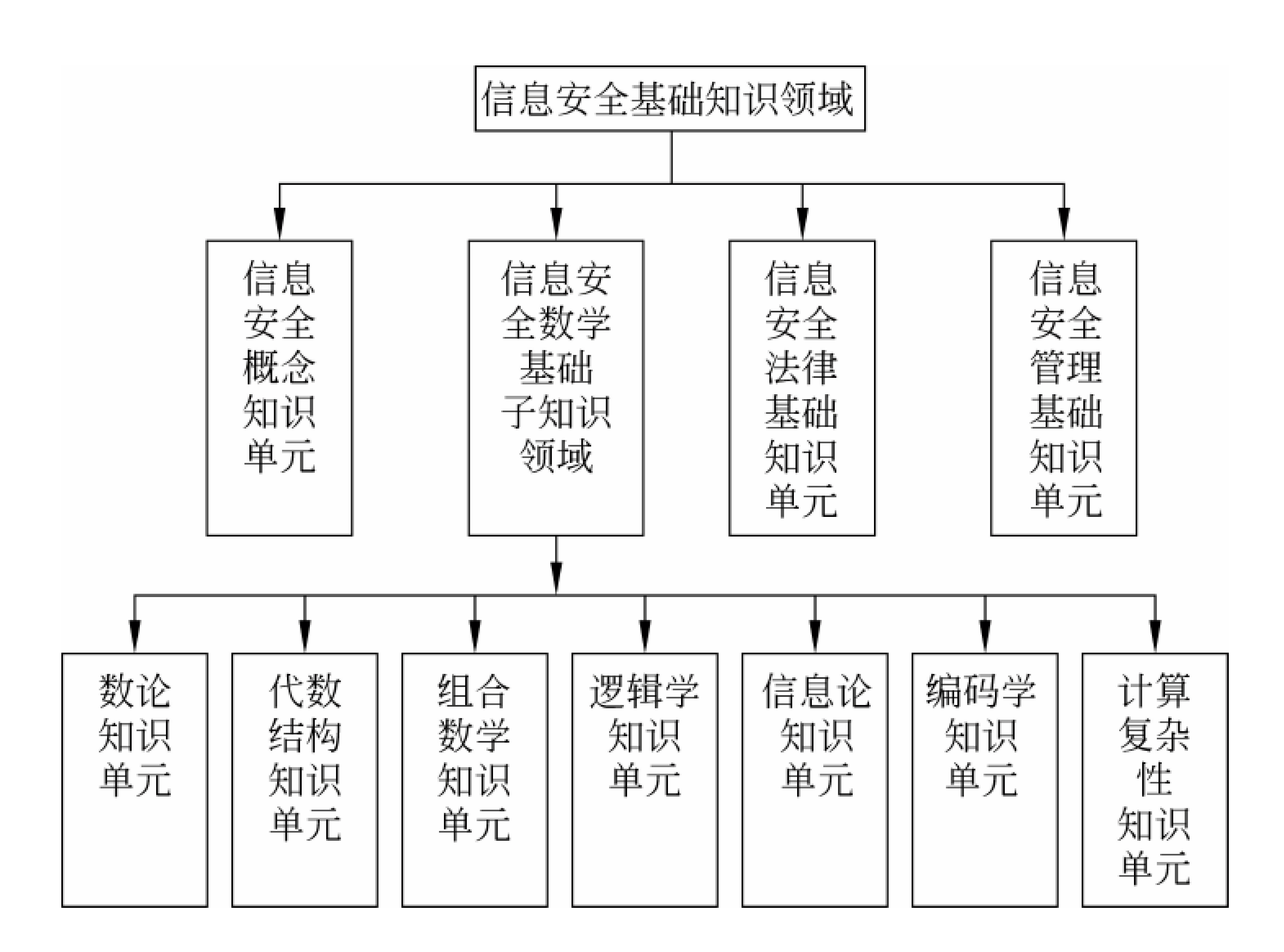


图 3-4　方案一的信息安全基础知识领域结构

ISB-1 信息安全概念

最少学时：4 学时

知识点：

- 信息安全的概念
- 信息安全威胁
- 信息安全问题的技术原因
- 确保信息安全的原则与措施

学习目标：

（1）掌握信息安全的概念；

（2）了解信息技术和产业的繁荣与信息安全威胁的挑战；

（3）了解产生信息安全问题的技术原因；

（4）了解确保信息安全的原则与措施；

（5）了解我国信息安全技术与产业的发展状况。

ISB-2 信息安全数学基础

数学是信息安全学科的理论基础之一，主要有代数、数论、概率

统计、组合数学、逻辑学和博弈论等。在本规范中，信息安全数学基础是一个子知识领域，下面设有数论、代数结构、组合数学（选修）、逻辑学（选修）、信息论（选修）、编码学（选修）和计算复杂性（选修），共7个知识单元。其中把信息论、编码学和计算复杂性放在这里的原因主要是考虑到它们具有较深入的数学理论，放在这里比放到其他知识领域下面更合适。

ISB-2-1 数论

最少学时：8学时

知识点：

- 素数与合数
- 同余性
- 整数的因子分解
- 欧拉定理
- 扩展欧几里得（Euclid）算法
- 中国剩余定理

学习目标：

（1）掌握整数的分类：合数和素数的概念；

（2）掌握整数的同余性概念和同余运算；

（3）掌握整数因子分解的概念，了解大整数因子分解的困难性；

（4）掌握欧拉定理及其基本应用；

（5）掌握扩展欧几里得算法及其基本应用；

（6）掌握中国剩余定理及其基本应用；

（7）了解数论在信息安全领域的应用。

ISB-2-2 代数结构

最少学时：24学时

知识点：

- 群：群、子群、交换群、循环群的定义和基本性质，群上的离散对数问题

- 环：环、子环、交换环的定义和基本性质，整数环，多项式环
- 域：域、子域、有限域的定义和基本性质，有限域的加法群，有限域的乘法群，有限域上的多项式

学习目标：

（1）掌握群、子群、交换群、循环群的定义及其基本性质与运算，熟悉一些常用群；

（2）掌握群上离散对数问题的概念；

（3）掌握环、子环、交换环的定义及其基本性质与运算，熟悉整数环、多项式环和理想子环；

（4）掌握域、子域和有限域的定义，有限域的基本性质、有限域的加法群，有限域的乘法群，熟悉一些常用的有限域；

（5）了解群、环、域在信息安全领域中的应用。

ISB-2-3 组合数学(选修)

最少学时：12 学时

知识点：

- 排列与组合
- 容斥原理
- 母函数
- 递推关系
- 区组设计

学习目标：

（1）掌握排列组合的概念和应用；

（2）掌握容斥原理，能应用它求解简单组合问题；

（3）掌握母函数的方法，能应用它求解简单组合问题；

（4）掌握递推关系，能应用它求解简单组合问题；

（5）了解区组设计的概念和应用；

（6）了解组合数学在信息安全领域中的应用。

ISB-2-4 逻辑学(选修)

最少学时:18 学时

知识点:

- 命题
- 联结词
- 命题公式及其等价与蕴涵
- 命题公式的合取范式与析取范式
- 命题逻辑推理
- 谓词
- 量词
- 谓词公式及其等价与蕴涵
- 谓词公式的合取范式与析取范式
- 谓词逻辑推理

学习目标:

(1) 掌握命题、联结词、命题公式及其等价与蕴涵性、命题公式的合取范式与析取范式、命题逻辑推理的概念;

(2) 掌握命题公式的等价与蕴含的判断、求解命题公式的合取范式与析取范式、命题逻辑推理的基本方法;

(3) 掌握谓词、量词、谓词公式及其等价与蕴涵、谓词公式的合取范式与析取范式、谓词逻辑推理的概念;

(4) 掌握谓词公式的等价与蕴含的判断、求解谓词公式的合取范式与析取范式、谓词逻辑推理的基本方法;

(5) 了解逻辑学在信息安全领域中的应用。

ISB-2-5 信息论(选修)

最少学时:18 学时

知识点:

- 通信系统模型

- 自信息、条件自信息、互信息
- 熵、条件熵、联合熵
- 保密系统模型
- 完善保密性
- 唯一解距离
- 乘积密码

学习目标：

(1) 熟悉解通信系统模型；

(2) 熟悉保密系统模型；

(3) 掌握自信息、条件自信息、互信息、熵、条件熵、联合熵的概念和基本性质；

(4) 掌握完善保密性、唯一解距离、乘积密码的概念；

(5) 了解信息论对密码学的基础作用。

ISB-2-6 编码学(选修)

最少学时：20 学时

知识点：

- 纠错编码的概念
- 差错控制技术
- 线性分组码：Hamming 码，最佳奇权码，GF（2^b）上的 Hamming 码
- 循环码：BCH 码，Fire 码，RS 码
- 卷积码
- 交错码
- 乘积码
- 纠错码在计算机系统中的应用
- 纠错码在通信系统中的应用
- 纠错码在信息安全领域中的应用

学习目标：

（1）掌握纠错编码的概念；

（2）掌握差错控制技术的概念；

（3）掌握线性分组码、Hamming 码、最佳奇权码、GF（2^b）上的 Hamming 码的概念与功能；

（4）掌握循环码、BCH 码、Fire 码、RS 码的概念与功能；

（5）熟悉卷积码的概念；

（6）掌握交错码和乘积码的概念；

（7）了解纠错码在计算机系统中的应用；

（8）了解纠错码在通信系统中的应用；

（9）了解纠错码在信息安全领域中的应用。

ISB-2-7 计算复杂性(选修)

最少学时：14 学时

知识点：

- 算法的时间复杂性
- 算法的空间复杂性
- 复杂性的渐进表示
- 问题的复杂性
- P 类问题
- NP 类问题
- NPC 类问题

学习目标：

（1）掌握算法的时间复杂性和空间复杂性的定义；

（2）掌握算法复杂性的渐进性表示，能够分析一些简单算法的时间复杂性和空间复杂性；

（3）掌握问题复杂性的概念；

（4）熟悉 P 类、NP 类、NPC 类问题的概念；

（5）了解一些常见的 NPC 问题；

（6）了解计算复杂性理论在信息安全领域中的应用。

ISB-3 信息安全法律基础

最少学时：8 学时

知识点：

- 信息安全法律、法规的概念
- 利用计算机犯罪
- 隐私权保护
- 数字知识产权
- 电子签名法

学习目标：

（1）掌握信息安全法律、法规的概念；

（2）掌握利用计算机犯罪的概念和特征；

（3）熟悉关于利用计算机犯罪的刑法规定；

（4）熟悉关于因特网安全的刑事责任；

（5）了解我国关于信息安全的一些法规和规章：主要包括《中华人民共和国计算机信息系统安全保护条例》、《中华人民共和国计算机信息网络国际联网管理暂行规定（修正）》、《计算机信息网络国际联网管理暂行规定实施办法》、《中华人民共和国计算机信息网络国际联网安全保护管理办法》、《计算机网络信息系统安全保密管理暂行规定》、《商用密码管理条例》、《计算机病毒防治管理条例》、《信息安全等级保护管理办法》等方面的法规和规章；

（6）掌握隐私权的基本概念，了解计算机和网络对隐私权的影响；

（7）熟悉知识产权的种类和概念，了解我国对计算机软件著作权、专利权的保护；

（8）了解《中华人民共和国电子签名法》，了解数据电文的法律地位以及关于电子签名与认证的法律规定。

ISB-4 信息安全管理基础

最少学时：8 学时

知识点：

- 信息安全管理的概念
- 信息安全风险评估与管理
- 信息安全产品测评与认证
- 商用密码产品管理
- 信息安全等级保护

学习目标：

（1）掌握信息安全管理的概念；

（2）熟悉信息安全管理的基本对象与管理办法（设备管理、信息管理、密码管理、网络管理、人员管理等）；

（3）掌握风险评估和风险管理的概念，了解风险评估的主要技术；

（4）了解我国信息安全产品测评与认证的政策和管理办法；

（5）了解我国信息安全等级保护的政策与管理办法；

（6）了解我国对商用密码产品的管理办法。

2. CRYPT 密码学（52 学时）

（1）CRYPT-1 密码学概念

（2）CRYPT-2 分组密码

（3）CRYPT-3 流密码

（4）CRYPT-4 Hash 函数

（5）CRYPT-5 公钥密码

（6）CRYPT-6 密码协议

(7) CRYPT-7 数字签名

(8) CRYPT-8 认证

(9) CRYPT-9 密钥管理

密码学由密码编制学和密码分析学组成。密码编制学研究编制高质量密码的理论与技术，密码分析学研究分析和破译密码的理论与技术。这两者相辅相成，共同组成密码学。

密码技术是信息安全领域的关键技术，而且是一种共性技术，许多信息安全领域都要用到密码技术。密码技术已经广泛应用于通信保密、信息系统安全、网络安全和信息内容安全等许多信息安全的重要领域中。

密码学的课程是信息安全专业的核心课程和主干课程，而且是一门典型的理论与实践相结合的课程。一方面，它是理论性比较深入的课程，需要有较多的数学知识作为学习的基础。另一方面，它也具有很强的实践性，密码算法的实现以及密码技术的应用都具有很强的实践性。

密码学的知识领域主要包括：密码学概念、分组密码、流密码、Hash函数、公钥密码、密码协议、数字签名、认证和密钥管理，共9个知识单元。

CRYPT-1 密码学概念

最少学时：4学时

知识点：

- 密码体制
- 古典密码
- 密码安全性

学习目标：

(1) 掌握密码技术的基本思想；

(2) 掌握密码体制的组成结构；

(3) 熟悉置换、代替和代数等基本古典密码的编码方法；

(4) 掌握密码体制的分类；

（5）掌握密码安全性的概念。

CRYPT-2 分组密码

最少学时：8 学时

知识点：

- 分组密码的概念
- DES
- AES
- SMS4
- 分组密码工作模式

学习目标：

（1）掌握分组密码的基本概念；

（2）掌握 DES（3DES）、AES、SMS4 密码算法；

（3）了解 DES（3DES）、AES、SMS4 密码的安全性；

（4）了解 DES（3DES）、AES、SMS4 密码的应用；

（5）掌握分组密码常用工作模式及其特点。

CRYPT-3 流密码

最少学时：6 学时

知识点：

- 流密码的概念
- 线性移位寄存器序列
- 非线性序列
- 伪随机序列评价
- 典型流密码

学习目标：

（1）掌握流密码的基本概念；

（2）掌握线性移位寄存器序列产生器的结构与序列的伪随机性；

（3）熟悉非线性序列的概念与基本产生方法；

（4）了解常用伪随机性评价方法；

（5）掌握一种典型流密码（如祖冲之密码、RC4 密码等）。

CRYPT-4 Hash 函数

最少学时：6 学时

知识点：

- Hash 函数的概念
- SHA-3 Hash 函数
- SM3 Hash 函数
- HMAC

学习目标：

（1）掌握 Hash 函数的基本概念和安全性要求；

（2）掌握 SHA-3 的算法；

（3）掌握 SM3 的算法；

（4）掌握 HMAC 的算法；

（5）了解 SHA-3 的安全性；

（6）了解 SM3 的安全性；

（7）了解 Hash 函数和 HMAC 的应用。

CRYPT-5 公钥密码

最少学时：8 学时

知识点：

- 公钥密码的概念
- RSA 密码
- ElGamal 密码
- 椭圆曲线密码

学习目标：

（1）掌握公钥密码的概念；

（2）熟悉公钥密码的基本工作方式；

（3）掌握 RSA 密码、ElGamal 密码和椭圆曲线密码（包括 SM2）的原理与算法；

（4）了解 RSA 密码、ElGamal 密码和椭圆曲线密码（包括 SM2）的安全性；

（5）了解 RSA 密码、ElGamal 密码和椭圆曲线密码（包括 SM2）的应用。

CRYPT-6 密码协议

最少学时：2 学时

知识点：

- 密码协议的概念
- 密码协议的安全问题

学习目标：

（1）掌握密码协议的概念；

（2）了解密码协议的安全问题；

（3）了解提高密码协议安全性的途径。

CRYPT-7 数字签名

最少学时：6 学时

知识点：

- 数字签名的概念
- RSA 密码数字签名
- ElGamal 密码数字签名
- 椭圆曲线密码（包括 SM2）数字签名

学习目标：

（1）掌握数字签名的概念；

（2）掌握基于 RSA 密码、基于 ElGamal 密码和基于椭圆曲线密码（包括 SM2）的数字签名方法；

(3) 了解基于 RSA 密码、基于 ElGamal 密码和基于椭圆曲线密码（包括 SM2）的数字签名的安全性；

(4) 了解数字签名的应用。

CRYPT-8 认证

最少学时：6 学时

知识点：

- 认证的概念
- 消息认证码
- 身份认证
- 站点认证
- 报文认证

学习目标：

(1) 掌握认证的基本概念；

(2) 掌握消息认证码的概念；

(3) 掌握基于 Hash 函数的消息认证码 HMAC 和基于分组密码的消息认证码的产生算法，了解它们的安全性；

(4) 掌握身份认证的概念和基本方法；

(5) 掌握站点认证、报文源认证、报文宿认证、报文顺序认证和报文内容认证的概念与方法；

(6) 了解认证技术的应用。

CRYPT-9 密钥管理

最少学时：6 学时

知识点：

- 密钥管理的概念
- 对称密码的密钥管理
- 公钥密码的密钥管理
- 公钥基础设施 PKI

学习目标：

（1）掌握密钥管理的概念；

（2）熟悉传统密码的密钥管理技术；

（3）熟悉公钥密码的密钥管理技术；

（4）了解公钥基础设施 PKI 的概念和应用。

3. ISS 信息系统安全（60 + 36 学时）

（1）ISS-1 信息系统安全概念

（2）ISS-2 信息系统设备安全

（3）ISS-3 信息系统可靠性技术

（4）ISS-4 访问控制

（5）ISS-5 操作系统安全

（6）ISS-6 数据库安全

（7）ISS-7 软件安全

（8）ISS-8 电子商务安全（选修）

（9）ISS-9 电子政务安全（选修）

（10）ISS-10 数字取证技术（选修）

（11）ISS-11 嵌入式系统安全

一般地，信息系统是指由硬件、软件和网络等设备构成，按照一定的应用目标和规则对信息进行采集、加工、存储、传输和处理的人机系统，为用户提供一定的服务。

传统的信息安全只强调信息本身的安全属性。信息论的基本原理告诉我们：信息不能脱离它的载体而孤立存在。因此，我们不能脱离信息系统而孤立地谈论信息安全。应当从信息系统的角度来考虑信息安全，从而导出信息系统安全的概念。

信息系统安全强调信息系统整体上的安全性，即从信息系统的设备安全、数据安全、内容安全和行为安全 4 个层面考虑信息安全。

由于本知识领域的内容较多，可能需要几门课程来覆盖这些知识。信息系统安全类的课程许多是信息安全专业的核心课程和主干课程。信息系统安全类课程在总体上的特点是技术性和实践性强，有些内容有较深入的理论性，多数内容则有很强的技术性。坚持理论联系实际，才能真正掌握这些知识。

通过信息系统安全类课程的学习，学生可以掌握信息系统安全的基本概念、基本理论与基本技术，结合实践锻炼使学生掌握分析和解决信息系统安全实际问题的基本能力。

信息系统安全的知识领域包括：信息系统安全概念、信息系统设备安全、信息系统可靠性技术、访问控制、操作系统安全、数据库安全、软件安全、电子商务安全（选修）、电子政务安全（选修）、数字取证技术（选修）和嵌入式系统安全，共 11 个知识单元。

ISS-1 信息系统安全概念

最少学时：4 学时

知识点：

- 信息系统安全的概念
- 确保信息系统安全的原则与措施
- 信息系统安全等级保护

学习目标：

（1）掌握信息系统安全的概念；

（2）熟悉确保信息系统安全的原则与措施；

（3）了解确保信息系统安全的技术措施（硬件、操作系统、密码、网络安全和数据库安全等）；

（4）熟悉信息系统安全等级保护的概念；

（5）了解信息系统安全等级保护的原则和基本技术。

ISS-2 信息系统设备安全

最少学时：4 学时

知识点：

- 信息系统设备安全的概念
- 信息系统设备的稳定性、可靠性和可用性
- 信息系统的环境安全：机房和场地安全

学习目标：

（1）掌握信息系统设备安全的概念；

（2）了解信息系统所面临的环境与设备安全的威胁；

（3）了解确保信息系统环境安全的基本原则；

（4）了解确保信息系统设备安全的基本原则。

ISS-3 信息系统可靠性技术

最少学时：8 学时

知识点：

- 信息系统稳定性、可靠性和可用性的概念
- 信息系统容错和容灾的概念
- 容错技术：硬件冗余、软件冗余、数据冗余和时间冗余
- 容灾技术

学习目标：

（1）掌握系统稳定性、可靠性和可用性的概念；

（2）掌握信息系统容错和容灾的概念；

（3）熟悉通过硬件冗余、软件冗余、数据冗余和时间冗余达到容错的基本原理和一些常用容错技术；

（4）了解容灾的基本原则和基本技术。

ISS-4 访问控制

最少学时：8 学时

知识点：

- 访问控制的概念
- 访问控制模型

- 访问控制技术
- 身份认证

学习目标：

（1）掌握访问控制的基本概念；

（2）掌握自主访问控制和强制访问控制的原理；

（3）掌握访问控制矩阵模型，熟悉 BLP 模型，了解 BRAC 模型；

（4）熟悉访问控制的基本技术；

（5）掌握身份认证的基本概念；

（6）掌握基于口令的身份认证技术，熟悉基于智能卡的身份认证技术或基于 USB-Key 的身份认证技术；

（7）了解访问控制技术在信息系统中的应用。

ISS-5 操作系统安全

最少学时：10＋2 学时

知识点：

- 操作系统安全的概念
- 操作系统中的访问控制技术
- 存储保护
- 文件保护
- 操作系统的安全审计
- 隐蔽通道的概念（选修）
- 主流操作系统的安全机制与配置

学习目标：

（1）掌握操作系统安全的概念；

（2）熟悉操作系统访问控制技术；

（3）掌握操作系统的存储保护、文件保护和安全审计的概念；

（4）熟悉存储保护技术、文件保护技术和安全审计技术；

（5）了解隐蔽通道的概念；

(6) 了解美国《可信计算机系统评价准则》(TCSEC) 和我国的国家标准 GB 17859—1999:《计算机信息系统安全保护等级划分准则》;

(7) 熟悉一种主流操作系统的安全机制,并能够进行安全配置。

ISS-6 数据库安全

最少学时: 10+2 学时

知识点:

- 数据库安全的概念
- 数据库的访问控制技术
- 数据库加密
- 数据库的备份与恢复
- 数据库的安全审计
- 主流数据库的安全机制与配置(选修)

学习目标:

(1) 掌握数据库安全的基本概念;

(2) 熟悉数据库的访问控制技术;

(3) 熟悉数据库的加密技术;

(4) 掌握数据库备份与恢复的概念,了解数据库备份与恢复的基本技术;

(5) 熟悉数据库安全审计的概念,了解数据库的安全审计技术;

(6) 了解一种主流数据库的安全机制与配置方法。

ISS-7 软件安全

最少学时: 10 学时

知识点:

- 软件安全的概念
- 软件的缺陷与漏洞
- 恶意代码的概念与原理

- 恶意代码的检测与防护
- 软件安全测试

学习目标：

（1）了解软件安全威胁；

（2）了解软件缺陷和漏洞存在的原因；

（3）掌握软件安全的概念；

（4）掌握恶意代码（病毒、蠕虫、木马等）的概念和基本机理；

（5）掌握恶意代码的检测与防护技术；

（6）了解软件安全测试的概念和基本技术。

ISS-8 电子商务安全（选修）

最少学时：10 学时

知识点：

- 电子商务安全的概念
- 电子商务中的安全问题与安全技术
- 电子商务安全协议

学习目标：

（1）掌握电子商务安全的概念；

（2）熟悉电子商务中的安全问题和主要安全技术；

（3）了解电子货币的概念；

（4）熟悉安全支付的基本技术；

（5）了解 SET 协议；

（6）了解一种电子商务系统的安全机制。

ISS-9 电子政务安全（选修）

最少学时：10 学时

知识点：

- 电子政务安全的概念
- 电子政务中的安全问题与安全技术

- 电子政务安全管理

学习目标：

（1）掌握电子政务安全的概念；

（2）了解我国电子政务建设的基本内容和网络规范；

（3）了解我国电子政务信息安全等级保护的基本内容；

（4）熟悉电子政务认证和权限管理的基本技术；

（5）了解电子政务信息交换的安全管理；

（6）了解我国政府应急平台的主要功能。

ISS-10 数字取证技术（选修）

最少学时：8 学时

知识点：

- 数字取证的概念
- 电子证据及其法律规定
- 数字取证技术

学习目标：

（1）了解证据的法律属性；

（2）掌握电子证据的概念，了解电子证据的相关法律规定；

（3）掌握数字取证的基本概念，了解数字取证的法律地位；

（4）熟悉数字取证的基本技术（如文件恢复、磁盘恢复等技术）；

（5）了解数字取证的应用。

ISS-11 嵌入式系统安全

最少学时：6＋4 学时

知识点：

- 嵌入式系统安全的概念
- 嵌入式系统设备
- 嵌入式系统安全技术
- 工业控制系统安全的概念（选修）

• 工业控制系统的安全技术（选修）

学习目标：

（1）了解嵌入式系统的安全威胁；

（2）掌握嵌入式系统安全的基本概念；

（3）掌握一种嵌入式系统设备（智能卡，USB-Key，智能移动终端）的安全功能与应用；

（4）熟悉一种嵌入式系统（智能卡，USB-Key，智能移动终端，等）的体系结构、工作原理、接口技术及其安全功能；

（5）熟悉嵌入式操作系统的结构及安全机制；

（6）掌握工业控制系统安全的概念；

（7）了解工业控制系统的基本安全技术。

4. NS 网络安全（44＋12 学时）

（1）NS-1 网络安全概念

（2）NS-2 防火墙

（3）NS-3 入侵检测系统（IDS）

（4）NS-4 虚拟专用网（VPN）

（5）NS-5 网络协议安全

（6）NS-6 网络防护

（7）NS-7 Web 安全

（8）NS-8 无线网络安全（选修）

网络是近代信息科学技术最辉煌的成就之一。网络已经成为人们生活和工作不可缺少的重要组成部分。网络为人们的生活和工作带来了便利，提高了生活质量和工作效率。与此同时，人们在使用网络时，也面临许多网络安全威胁，如黑客攻击、病毒与木马的入侵、敏感信息泄漏、网络欺诈，等等。以至于人们常说：如果你使用网络，你受到信息安全危害的可能性将增大 10 倍。可是你不使用网络，你所得到的信息服务将减小 10

倍。今天，危害信息安全的主要威胁来自基于网络的攻击。近年来，无线网络迅速发展，并得到广泛应用。由于无线信号的辐射特性，使得无线网络安全问题更加突出。因此，网络安全成为信息安全的重要内容之一。

由于本知识领域的内容较多，可能需要几门课程来覆盖这些知识。网络安全课程是信息安全专业的核心课程和主干课程。网络安全课程在总体上的特点是技术性和实践性强。有些内容有较深入的理论性，多数内容则有很强的技术性。如深入学习网络协议安全需要较多的逻辑学等数学知识，而防火墙、入侵检测和 Web 安全等都有很强的技术性。坚持理论联系实际，才能真正掌握这些知识。

通过学习网络安全，学生将可以了解网络安全的威胁，掌握入侵检测、安全防护以及应急响应等基本安全技术，可以为信息系统的设计和实现提供网络安全防御机制，从系统的整个生命周期考虑网络安全问题，从而提高信息系统的安全性。

网络安全的知识领域包括：网络安全概念、防火墙、入侵检测系统（IDS）、虚拟专用网（VPN）、网络协议安全、网络防护、Web 安全和无线网络安全（选修），共 8 个知识单元。

NS-1 网络安全概念

最少学时：4 学时

知识点：

- 网络安全威胁
- 网络安全评估
- 安全事件响应
- 网络安全模型

学习目标：

（1）掌握网络安全的概念；

（2）掌握病毒木马等恶意软件和黑客攻击对网络安全威害的基本原理；

(3) 了解网络安全评估的概念和基本技术；

(4) 熟悉网络安全的 P^2DR 模型；

(5) 了解网络安全的基本保障技术与方法；

(6) 了解网络安全事件的基本处置方法。

NS-2 防火墙

最少学时：6 学时

知识点：

- 防火墙的概念
- 防火墙的技术

学习目标：

(1) 掌握防火墙的基本概念、构成和分类；

(2) 掌握包过滤、应用层代理、电路级网关和 NAT 技术；

(3) 了解防火墙规则配置原理。

NS-3 入侵检测系统（IDS）

最少学时：6 学时

知识点：

- 入侵检测的概念
- 误用检测
- 异常检测

学习目标：

(1) 掌握入侵检测的基本概念；

(2) 了解入侵检测系统的分类（NIDS 和 HIDS）和基本结构；

(3) 掌握异常检测和误用检测的原理；

(4) 了解入侵检测系统的应用与部署。

NS-4 虚拟专用网（VPN）

最少学时：8 学时

知识点：

- 虚拟专用网的概念
- 虚拟专用网的安全技术
- 虚拟专用网的协议

学习目标：

（1）掌握虚拟专用网的基本概念；

（2）熟悉虚拟专用网的加密技术；

（3）熟悉虚拟专用网采用的典型安全协议，如 IPSec 等；

（4）了解虚拟专用网的应用与部署。

NS-5 网络协议安全

最少学时：6 学时

知识点：

- 网络协议安全的基本概念
- 典型的网络安全协议

学习目标：

（1）了解网络协议的安全问题；

（2）掌握网络协议安全的概念；

（3）熟悉一种典型网络安全协议（如 Kerberos，Open SSL 等协议）及其应用；

（4）了解提高网络协议安全性的措施。

NS-6 网络防护

最少学时：8 学时

知识点：

- 网络攻击与防护的概念
- 网络安全扫描技术
- 网络隔离技术
- 恶意代码防护

• 邮件安全防护
• 网络安全审计

学习目标：

（1）掌握网络攻击与防护的概念；
（2）了解 TCP/IP 的安全漏洞与威胁；
（3）熟悉安全扫描技术（端口扫描和漏洞扫描），能够使用常用安全扫描工具；
（4）掌握网络隔离的概念与原理；
（5）熟悉防火墙、网闸和 VLAN 技术等网络隔离技术的原理和方法；
（6）熟悉网络环境中的恶意代码防护技术，掌握一种恶意代码查杀工具的应用；
（7）了解邮件安全风险，掌握邮件安全检测的基本方法；
（8）了解网络安全审计技术。

NS-7 Web 安全

最少学时：6 学时

知识点：

• Web 安全威胁
• Web 安全防护技术

学习目标：

（1）了解 Web 安全威胁和防御方法；
（2）了解 HTTPS 协议；
（3）熟悉 Web 认证技术；
（4）熟悉网页过滤和防篡改的基本原理。

NS-8 无线网络安全（选修）

最少学时：12 学时

知识点：

- 无线网络的安全弱点
- 无线网络安全策略
- 无线网络安全协议
- 无线网络接入安全
- 移动通信网络安全

学习目标：

（1）掌握无线网络安全的概念；

（2）了解无线网络的安全弱点；

（3）熟悉无线网络安全策略的制定和实施；

（4）熟悉无线通信网络的数据加密、认证技术和授权技术；

（5）了解无线网络安全协议；

（6）了解无线接入网络安全问题与基本技术（如 WLAN 等）；

（7）了解移动通信网络安全问题与基本技术(如 2G/3G/4G 等)。

5. ICS 信息内容安全(8+38 学时)

（1）ICS-1 信息内容安全概念

（2）ICS-2 网络数据的获取

（3）ICS-3 信息内容的分析与识别（选修）

（4）ICS-4 信息内容的管控（选修）

（5）ICS-5 多媒体信息隐藏（选修）

（6）ICS-6 隐私保护（选修）

信息内容安全是信息安全在法律、政治、道德层次上的要求。我们要求信息内容是安全的，就是要求信息内容在政治上是健康的，在法律上是符合国家法律法规的，在道德上是符合中华民族优良的道德规范的。确保信息内容安全旨在获取数据，分析信息内容是否符合我国法律、政治、道德的要求，确保合法内容的安全，阻止非法内容的传播和利用。

目前学术界对信息内容安全的认识尚不一致。广义的信息内容安全既

包括信息内容在政治、法律和道德方面的要求，也包括信息内容的保密、知识产权保护、信息隐藏、隐私保护等诸多方面。

信息隐藏技术是一种把一个秘密信息隐藏到另一载体中去，并使未授权者不易感知和获取这一个秘密信息的技术。信息隐藏技术可以分为隐蔽信道技术和多媒体信息隐藏技术。隐蔽信道技术利用各种隐蔽信道来实现秘密信息的隐藏和传输。多媒体信息隐藏以多媒体信号为载体，利用多媒体数据的数据冗余和人们的听视觉冗余来隐藏秘密信息。与信息隐藏对立的技术称为信息隐藏分析技术，研究如何攻击信息隐藏以获取所隐藏的秘密信息。信息隐藏不同于密码技术。密码技术把秘密信息编码成不被识别的密文，以达到信息保密的目的。而信息隐藏则是把秘密信息隐藏到另一载体中，以达到信息保密的目的。显然，密码技术和信息隐藏技术都是信息内容保护技术，但是两种技术各有不同的优缺点。

隐私是不愿意公开或不愿意告诉别人的个人信息。公民享有隐私权。世界上许多国家都颁布了相关的法律，保护公民的隐私权。但是随着社会的信息化，网络上的个人信息越来越多，危害公民隐私权、泄漏公民隐私的事件也越来越多。保护公民隐私权，除了采用法律保护之外，还必须采用技术手段进行保护。

我们在这里既考虑信息内容在政治、法律和道德方面的要求，也考虑信息隐藏和隐私保护等方面的要求。而且强调信息内容安全中的基本概念、基本理论和基本技术。

通过学习信息内容安全，学生将可以了解信息内容安全的威胁，掌握信息内容安全的基本概念、基本理论、基本技术和基本应用。

信息内容安全的知识领域包括：信息内容安全概念，网络数据的获取，信息内容的分析与识别(选修)，信息内容的管控(选修)，多媒体信息隐藏(选修)，隐私保护(选修)，共6个知识单元。

ICS-1 信息内容安全概念

最少学时： 2学时

知识点：

- 信息内容安全的概念
- 信息内容安全的威胁
- 确保信息内容安全的措施

学习目标：

（1）掌握信息内容安全的概念；

（2）了解信息内容安全的威胁；

（3）了解确保信息内容安全的技术措施与法律法规保障。

ICS-2 网络数据的获取

最少学时：6 学时

知识点：

- 网络数据获取的概念
- 网络数据的被动获取技术
- 网络数据的主动获取技术
- 网络协议还原技术

学习目标：

（1）掌握网络数据获取的概念；

（2）掌握常用的网络数据被动获取技术；

（3）熟悉常用的网络数据主动获取技术；

（4）掌握一种网络协议还原技术；

（5）了解网络数据获取技术的应用。

ICS-3 信息内容的分析与识别（选修）

最少学时：6 学时

知识点：

- 信息内容分析与识别的概念
- 基于文本的特征串匹配技术
- 文本分类技术

- 数据挖掘技术

学习目标：

（1）掌握信息内容识别的概念；

（2）掌握一种基于文本的特征串匹配技术（单模式匹配，多模式匹配等匹配算法）；

（3）熟悉一种常用的数据挖掘技术；

（4）了解信息内容识别技术的应用。

ICS-4 信息内容的管控（选修）

最少学时：6 学时

知识点：

- 信息内容安全管控的概念
- 基于网络地址的阻断技术
- 基于内容的阻断技术
- 信息内容管控的相关法律法规

学习目标：

（1）掌握信息内容安全管控的概念；

（2）掌握基于网络地址（IP 地址，域名）的阻断技术；

（3）了解基于内容的阻断技术；

（4）了解信息内容管控相关的法律法规；

（5）了解信息内容管控技术的应用。

ICS-5 多媒体信息隐藏（选修）

最少学时：18 学时

知识点：

- 信息隐藏的概念
- 多媒体信息隐藏的概念与基本技术
- 隐写的概念与基本技术
- 数字水印的概念与基本技术

- 数字指纹的概念与基本技术
- 数字权益管理

学习目标：

（1）掌握信息隐藏的概念；

（2）掌握多媒体信息隐藏的基本原理与技术；

（3）了解隐写的基本原理与技术；

（4）掌握数字水印的基本原理与技术；

（5）了解数字指纹的基本原理与技术；

（6）掌握数字权益管理的概念，了解常用数字权益管理技术。

ICS-6 隐私保护（选修）

最少学时：8 学时

知识点：

- 隐私和隐私保护的概念
- 社会信息化对公民隐私的威胁
- 隐私保护的基本原理
- 隐私保护技术（如匿名技术，磁盘加密技术，磁盘数据擦除技术等）
- 隐私保护的法律保障

学习目标：

（1）掌握隐私和隐私保护的概念；

（2）了解社会信息化对公民隐私的威胁；

（3）掌握隐私保护的基本原理；

（4）熟悉隐私保护技术的综合性特点，掌握一种隐私保护技术；

（5）了解我国隐私保护的法律法规。

3.4.4 知识体系方案二

本专业规范遵循分类指导的原则，制定出一个规范，提供两套方案。

各高校可以根据自己的实际情况，自主选用，而且在选择之后还可以更换。

方案一：培养学生以从事信息安全领域的研究开发工作为主。

方案二：培养学生以从事信息安全领域的应用服务工作为主。

1. ISB 信息安全基础(28 学时)

(1) ISB-1 信息安全概念

(2) ISB-2 信息安全数学基础

(3) ISB-3 信息安全法律基础

(4) ISB-4 信息安全管理基础

信息安全基础是信息安全学科的一些基础内容。信息安全基础知识领域由信息安全概念知识单元、信息安全数学基础知识单元、信息安全法律基础知识单元和信息安全管理基础知识单元，4 个部分组成。图 3-5 示出了它们之间的结构。

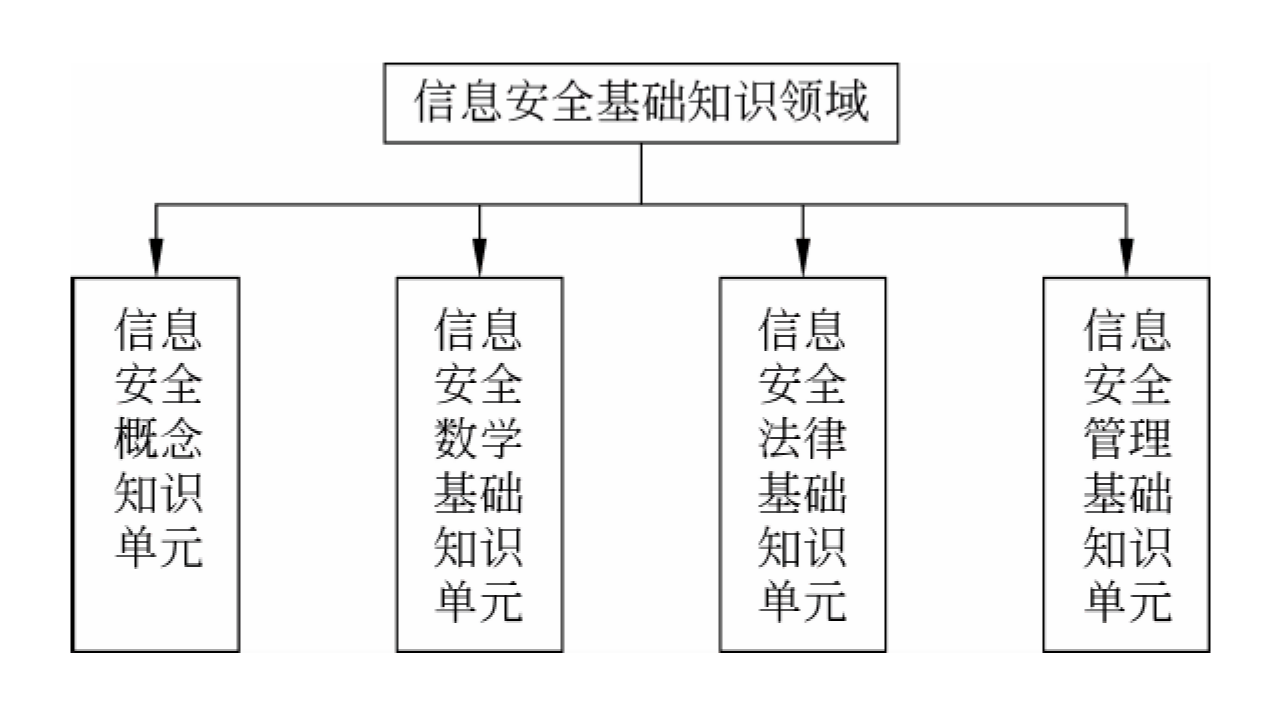


图 3-5 方案二的信息安全基础知识领域结构

信息安全基础中的信息安全概念主要介绍对信息安全的威胁、信息安全的基本概念和确保信息安全的措施等基本知识。信息安全数学是信息安全学科的理论基础之一，与方案一相比这里作了较大的裁减。信息安全法律基础介绍信息安全领域中的一些基本法律知识和我国在信息安全领域的主要法律法规。信息安全管理基础介绍信息安全领域中的一些基本管理知

识和方法。信息安全法律和信息安全管理知识则是对整个信息安全系统的设计、实现与应用具有指导性作用。

ISB-1 信息安全概念

最少学时：4 学时

知识点：

- 信息安全的概念
- 信息安全威胁
- 信息安全问题的技术原因
- 确保信息安全的原则与措施

学习目标：

（1）掌握信息安全的概念；

（2）了解信息技术和产业的繁荣与信息安全威胁的挑战；

（3）了解产生信息安全问题的技术原因；

（4）了解确保信息安全的原则与主要措施；

（5）了解我国信息安全技术与产业的发展状况。

ISB-2 信息安全数学基础

最少学时：8 学时

知识点：

- 素数与合数
- 同余性
- 整数的因子分解
- 欧拉定理
- 扩展欧几里得（Euclid）算法
- 中国剩余定理

学习目标：

（1）掌握合数和素数的定义；

（2）掌握整数的同余性及同余运算；

（3）掌握整数因子分解的概念，了解大整数因子分解的困难性；

（4）掌握欧拉定理；

（5）熟悉扩展欧几里得算法和中国剩余定理；

（6）了解数论在信息安全中的应用。

ISB-3 信息安全法律基础

最少学时：8 学时

知识点：

- 信息安全法律、法规的概念
- 利用计算机犯罪
- 隐私权保护
- 数字知识产权
- 电子签名法

学习目标：

（1）掌握信息安全法律、法规的概念；

（2）掌握利用计算机犯罪的概念和特征；

（3）熟悉关于利用计算机犯罪的刑法规定；

（4）熟悉关于因特网安全的刑事责任；

（5）了解我国关于信息安全的一些法规和规章：主要包括《中华人民共和国计算机信息系统安全保护条例》、《中华人民共和国计算机信息网络国际联网管理暂行规定（修正）》、《计算机信息网络国际联网管理暂行规定实施办法》、《中华人民共和国计算机信息网络国际联网安全保护管理办法》、《计算机网络信息系统安全保密管理暂行规定》、《商用密码管理条例》、《计算机病毒防治管理条例》、《信息安全等级保护管理办法》等方面的法规和规章；

（6）掌握隐私权的基本概念，了解计算机和网络对隐私权的

影响；

(7) 熟悉知识产权的种类和概念，了解我国对计算机软件著作权、专利权的保护；

(8) 了解《中华人民共和国电子签名法》，了解数据电文的法律地位以及关于电子签名与认证的法律规定。

ISB-4 信息安全管理基础

最少学时：8 学时

知识点：

- 信息安全管理的概念
- 信息安全风险评估与管理
- 信息安全产品测评与认证
- 商用密码产品管理
- 信息安全等级保护

学习目标：

(1) 掌握信息安全管理的概念；

(2) 熟悉信息安全管理的基本对象与管理办法（设备管理、密码管理、网络管理和人员管理等）；

(3) 掌握风险评估和风险管理的概念，了解风险评估的主要技术；

(4) 了解我国信息安全产品测评与认证的政策和管理办法；

(5) 了解我国信息安全等级保护的政策与管理办法；

(6) 了解我国商业密码产品的管理办法。

2. CRYPT 密码学(34 学时)

(1) CRYPT-1 密码学概念

(2) CRYPT-2 分组密码

(3) CRYPT-3 流密码

(4) CRYPT-4 Hash 函数
(5) CRYPT-5 公钥密码
(6) CRYPT-6 密码协议
(7) CRYPT-7 数字签名
(8) CRYPT-8 认证
(9) CRYPT-9 密钥管理

密码学由密码编制学和密码分析学组成。密码编制学研究编制高质量密码的理论与技术，密码分析学研究分析和破译密码的理论和技术。这两者相辅相成，共同组成密码学。

密码技术是信息安全领域的关键技术，而且是一种共性技术，许多信息安全领域都用到密码技术。密码技术已经广泛应用于通信保密、信息系统安全、网络安全和信息内容安全等许多信息安全的重要领域中。

密码学是信息安全专业的核心课程和主干课程。密码学是一门典型的理论与实践相结合的课程。一方面，它是理论性比较深入的课程，需要有较多的数学知识作为学习的基础。另一方面，它也具有很强的实践性，密码算法的实现以及密码学的应用都具有很强的实践性。

作为本规范中方案二的密码学知识领域，重点学习密码学的一些基本概念和典型密码算法，强调密码技术的实现与应用。与方案一相比，方案二作了较大的裁剪。

密码学的知识领域主要包括：密码学概念、分组密码、流密码、Hash 函数、公钥密码、密码协议、数字签名、认证、密钥管理，共 9 个知识单元。

CRYPT-1 密码学概念

最少学时：4 学时

知识点：

- 密码体制
- 古典密码

- 密码安全性

学习目标：

（1）掌握密码技术的基本思想；

（2）熟悉密码体制的分类；

（3）了解几种古典密码；

（4）了解密码的安全性。

CRYPT-2 分组密码

最少学时：6 学时

知识点：

- 分组密码的概念
- 常用分组密码算法
- 分组密码的工作模式

学习目标：

（1）掌握分组密码的基本概念；

（2）掌握一种常用分组密码算法，如 SMS4 或 AES 或 3DES；

（3）熟悉分组密码常用工作模式及其特点。

CRYPT-3 流密码

最少学时：2 学时

知识点：

- 流密码的概念
- 常用流密码算法

学习目标：

（1）掌握流密码的基本概念；

（2）掌握一种常用流密码算法（如祖冲之密码或 RC4）。

CRYPT-4 Hash 函数

最少学时：4 学时

知识点：

- Hash 函数概念
- 常用 Hash 函数

学习目标：

（1）掌握 Hash 函数的基本概念；

（2）熟悉一种常用 Hash 函数，如 SM3 或 SHA-3 等 Hash 函数。

CRYPT-5 公钥密码

最少学时：4 学时

知识点：

- 公钥密码的概念
- RSA 密码

学习目标：

（1）掌握公钥密码的基本概念；

（2）熟悉 RSA 密码算法；

（3）了解 RSA 密码的应用。

CRYPT-6 密码协议

最少学时：2 学时

知识点：

- 密码协议的概念
- 密码协议的安全问题

学习目标：

（1）掌握密码协议的基本概念；

（2）了解密码协议的安全问题。

CRYPT-7 数字签名

最少学时：4 学时

知识点：

- 数字签名的概念
- RSA 密码数字签名

学习目标：

（1）掌握数字签名的基本概念；

（2）熟悉基于 RSA 密码的数字签名方法；

（3）了解数字签名的应用。

CRYPT-8 认证

最少学时：4 学时

知识点：

- 认证概念
- 身份认证

学习目标：

（1）掌握认证的基本概念；

（2）掌握一种身份认证方法。

CRYPT-9 密钥管理

最少学时：4 学时

知识点：

- 密钥管理的概念
- 公钥基础设施 PKI

学习目标：

（1）掌握密钥管理的基本概念；

（2）熟悉 PKI 技术；

（3）了解 PKI 的应用。

3. ISS 信息系统安全（60＋38 学时）

（1）ISS-1 信息系统安全概念

(2) ISS-2 信息系统设备安全

(3) ISS-3 信息系统可靠性技术

(4) ISS-4 访问控制

(5) ISS-5 操作系统安全

(6) ISS-6 数据库安全

(7) ISS-7 软件安全

(8) ISS-8 电子商务安全（选修）

(9) ISS-9 电子政务安全（选修）

(10) ISS-10 数字取证技术（选修）

(11) ISS-11 嵌入式系统安全

一般地，信息系统是指由硬件、软件和网络等设备构成，按照一定的应用目标和规则对信息进行采集、加工、存储、传输和处理的人机系统，为用户提供一定的功能服务。

传统的信息安全只强调信息本身的安全属性。信息论的基本原理告诉我们：信息不能脱离它的载体而孤立存在。因此，不能脱离信息系统而孤立地谈论信息安全，应当从信息系统的角度来考虑信息安全，从而导出信息系统安全的概念。

信息系统安全强调信息系统整体上的安全性，即从信息系统的设备安全、数据安全、内容安全和行为安全 4 个层面上来考虑信息安全。

由于本知识领域的内容较多，可能需要几门课程来覆盖这些知识。信息系统安全类的课程许多是信息安全专业的核心课程和主干课程。信息系统安全类课程在总体上的特点是技术性和实践性强，有些内容有较深入的理论性，多数内容则有很强的技术性。坚持理论联系实际，才能真正掌握这些知识。

通过信息系统安全类课程的学习，学生可以掌握信息系统安全的基本概念、基本理论与基本技术，结合实践锻炼使学生掌握分析和解决信息系统安全实际问题的基本能力。

信息系统安全的知识领域包括：信息系统安全概念、信息系统设备安全、信息系统可靠性技术、访问控制、操作系统安全、数据库安全、软件安全、电子商务安全（选修）、电子政务安全（选修）、数字取证技术（选修）和嵌入式系统安全，共 11 个知识单元。

对于本规范的方案二，在这里更强调了相关技术应用性知识单元，适当减少了部分理论性知识单元或适当降低了要求。

ISS-1 信息系统安全概念

最少学时：4 学时

知识点：

- 信息系统安全的概念
- 确保信息系统安全的原则与措施
- 信息系统安全等级保护

学习目标：

（1）熟悉信息系统安全的概念；

（2）了解确保信息系统安全的原则与措施；

（3）了解确保信息系统安全的技术措施（硬件、操作系统、密码、网络安全和数据库安全等）；

（4）熟悉信息系统安全等级保护的概念；

（5）了解信息系统安全等级保护的原则和基本技术。

ISS-2 信息系统设备安全

最少学时：4 学时

知识点：

- 信息系统设备安全的概念
- 信息系统设备的稳定性、可靠性和可用性
- 信息系统的环境安全：机房和场地安全

学习目标：

（1）掌握信息系统设备安全的概念；

（2）了解信息系统所面临的环境与设备安全的威胁；

（3）了解确保信息系统环境安全的基本原则；

（4）了解确保信息系统设备安全的基本原则。

ISS-3 信息系统可靠性技术

最少学时：8 学时

知识点：

- 信息系统稳定性、可靠性和可用性的概念
- 信息系统容错和容灾的概念
- 容错技术：硬件冗余、软件冗余、数据冗余和时间冗余
- 容灾技术

学习目标：

（1）掌握系统稳定性、可靠性和可用性的概念；

（2）掌握信息系统容错和容灾的概念；

（3）了解通过硬件冗余、软件冗余、数据冗余和时间冗余达到容错的基本原理和一些常用容错技术；

（4）了解容灾的基本原则与基本技术。

ISS-4 访问控制

最少学时：6＋2 学时

知识点：

- 访问控制的概念
- 自主访问控制模型
- 强制访问控制模型（选修）
- 身份认证

学习目标：

（1）掌握访问控制的基本概念；

（2）熟悉自主访问控制的概念和原理；

（3）了解强制访问控制的概念和原理；

（4）了解访问控制技术在信息系统中的应用；

（5）熟悉基于口令的身份认证技术，了解基于智能卡的身份认证或基于 USB-Key 的身份认证。

ISS-5 操作系统安全

最少学时：10＋2 学时

知识点：

- 操作系统安全的概念
- 操作系统访问控制技术
- 存储保护
- 文件保护
- 操作系统的安全审计
- 隐蔽通道的概念（选修）
- 主流操作系统的安全机制与配置

学习目标：

（1）掌握操作系统安全的概念；

（2）熟悉操作系统访问控制技术；

（3）掌握操作系统的存储保护、文件保护和安全审计的概念；

（4）了解存储保护技术、文件保护技术和安全审计技术；

（5）了解隐蔽通道概念；

（6）了解美国《可信计算机系统评价准则》（TCSEC）和我国的国家标准 GB 17859—1999：《计算机信息系统安全保护等级划分准则》；

（7）熟悉一种主流操作系统的安全机制，并能够进行安全配置。

ISS-6 数据库安全

最少学时：10＋2 学时

知识点：

- 数据库安全的概念

- 数据库的访问控制技术
- 数据库加密
- 数据库的备份与恢复
- 数据库的安全审计
- 主流数据库的安全机制与配置（选修）

学习目标：

（1）掌握数据库安全的基本概念；

（2）了解数据库的访问控制技术；

（3）了解数据库的加密技术；

（4）掌握数据库备份与恢复的概念，熟悉数据库备份与恢复的基本技术与应用；

（5）熟悉数据库安全审计的基本技术与应用；

（6）了解一种主流数据库的安全机制与配置方法。

ISS-7 软件安全

最少学时：10 学时

知识点：

- 软件安全的概念
- 软件的缺陷与漏洞
- 恶意代码的概念与原理
- 恶意代码的检测与防护
- 软件安全测试

学习目标：

（1）了解软件安全威胁；

（2）了解软件缺陷和漏洞存在的原因；

（3）掌握软件安全的概念；

（4）掌握恶意代码（病毒、蠕虫、木马等）的概念和机理；

（5）掌握恶意代码的基本防护技术；

（6）了解软件安全测试的概念和基本技术。

ISS-8 电子商务安全（选修）

最少学时：10 学时

知识点：

- 电子商务安全的概念
- 电子商务中的安全问题与安全技术
- 电子商务安全协议

学习目标：

（1）掌握电子商务安全的概念；

（2）熟悉电子商务中的安全问题和主要安全技术；

（3）了解电子货币的概念；

（4）熟悉安全支付的基本技术；

（5）了解 SET 协议；

（6）了解一种电子商务系统的安全机制。

ISS-9 电子政务安全（选修）

最少学时：10 学时

知识点：

- 电子政务安全的概念
- 电子政务中的安全问题与安全技术
- 电子政务安全管理

学习目标：

（1）掌握电子政务安全的概念；

（2）了解我国电子政务建设的基本内容和网络规范；

（3）熟悉我国电子政务信息安全等级保护的基本内容；

（4）熟悉电子政务认证和权限管理的应用；

（5）了解电子政务信息交换的安全管理；

（6）了解我国政府应急平台的主要内容。

ISS-10 数字取证技术（选修）

最少学时：8 学时

知识点：

- 数字取证的概念
- 电子证据及其法律规定
- 数字取证技术

学习目标：

（1）了解证据的法律属性；

（2）掌握电子证据的概念，了解电子证据的相关法律规定；

（3）掌握数字取证的基本概念，了解数字取证的法律地位；

（4）熟悉数字取证的基本技术（如文件恢复、磁盘恢复等技术）；

（5）了解数字取证的应用。

ISS-11 嵌入式系统安全

最少学时：8＋4 学时

知识点：

- 嵌入式系统安全的概念
- 嵌入式系统设备
- 嵌入式系统安全技术
- 工业控制系统安全的概念（选修）
- 工业控制系统的安全技术（选修）

学习目标：

（1）了解嵌入式系统的安全威胁；

（2）掌握嵌入式系统安全的基本概念；

（3）掌握一种嵌入式系统设备（智能卡，USB-Key，智能移动终端）的安全功能与应用；

（4）熟悉一种嵌入式系统（智能卡，USB-Key，智能移动终端等）的体系结构、工作原理、接口技术及其安全功能；

（5）了解嵌入式操作系统的结构及安全机制；
（6）熟悉一种嵌入式系统的应用开发技术；
（7）掌握工业控制系统安全的概念；
（8）了解工业控制系统的基本安全技术。

4. NS 网络安全(44+12 学时)

（1）NS-1 网络安全概念
（2）NS-2 防火墙
（3）NS-3 入侵检测系统（IDS）
（4）NS-4 虚拟专用网（VPN）
（5）NS-5 网络协议安全
（6）NS-6 网络防护
（7）NS-7 Web 安全
（8）NS-8 无线网络安全（选修）

网络是近代信息科学技术最辉煌的成就之一。网络已经成为人们生活和工作不可缺少的重要组成部分。网络为人们的生活和工作带来了便利，提高了生活质量和工作效率。与此同时，人们在使用网络时，也面临许多网络安全威胁，如恶意访问、敏感信息泄露、黑客入侵和拒绝服务攻击，等等。以至于人们常说：如果你使用网络，你受到信息安全危害的可能性将增大 10 倍。可是你不使用网络，你所得到的信息服务将减小 10 倍。今天，危害信息安全的主要威胁来自基于网络的攻击。近年来，无线网络迅速发展，并得到广泛应用。由于无线信号的辐射特性，使得无线网络安全问题更加突出。因此，网络安全成为信息安全的重要内容之一。

由于本知识领域的内容较多，可能需要几门课程来覆盖这些知识。网络安全课程是信息安全专业的核心课程和主干课程。网络安全课程在总体上的特点是技术性和实践性强。有些内容有较深入的理论性，多数内容则有很强的技术性。如深入学习网络协议安全需要较多的逻辑学等数学知

识，而防火墙、入侵检测和 Web 安全等都有很强的技术性。坚持理论联系实际，才能真正掌握这些知识。

通过学习网络安全，学生将可以了解网络安全的威胁，掌握入侵检测、安全防护以及应急响应等基本安全技术，可以为信息系统的设计和实现提供网络安全防御机制，从系统的整个生命周期考虑网络安全问题，从而提高信息系统的安全性。

网络安全的知识领域包括：网络安全概念、防火墙、入侵检测系统(IDS)、虚拟专用网（VPN)、网络协议安全、网络防护、Web 安全和无线网络安全（选修)，共 8 个知识单元。

与方案一相比，方案二的要求有所调整。在方案二中更强调了相关技术应用性知识单元，适当减少了部分知识单元中的理论性内容或适当降低了要求。

NS-1 网络安全概念

最少学时：4 学时

知识点：

- 网络安全威胁
- 网络安全评估
- 安全事件响应
- 网络安全模型

学习目标：

(1) 掌握网络安全的概念；

(2) 掌握病毒木马等恶意软件和黑客攻击对网络安全威害的基本原理；

(3) 了解网络安全评估的概念和基本技术；

(4) 了解网络安全的 P^2DR 模型；

(5) 了解网络安全的基本保障技术与方法；

(6) 熟悉网络安全事件的基本处置方法。

NS-2 防火墙

最少学时：6 学时

知识点：

- 防火墙的概念
- 防火墙的技术

学习目标：

(1) 掌握防火墙的基本概念；

(2) 了解包过滤、应用层代理、电路级网关和 NAT 技术；

(3) 了解防火墙的优点与局限性；

(4) 掌握一种防火墙的配置方法，能够正确配置防火墙。

NS-3 入侵检测系统(IDS)

最少学时：6 学时

知识点：

- 入侵检测的概念
- 误用检测
- 异常检测

学习目标：

(1) 掌握入侵检测的基本概念；

(2) 了解入侵检测系统的分类（NIDS 和 HIDS）和基本结构；

(3) 掌握异常检测和误用检测的原理；

(4) 了解入侵检测的优点与局限性；

(5) 掌握入侵检测系统的配置方法，能够正确配置一种入侵检测系统。

NS-4 虚拟专用网(VPN)

最少学时：8 学时

知识点：

- 虚拟专用网的概念
- 虚拟专用网的安全技术
- 虚拟专用网的协议

学习目标：

（1）掌握虚拟专用网的基本概念；

（2）熟悉虚拟专用网的安全技术；

（3）了解虚拟专用网采用的典型安全协议，如 IPSec 等；

（4）掌握虚拟专用网设备的配置方法，能够正确配置一种虚拟专用网设备。

NS-5 网络协议安全

最少学时：6 学时

知识点：

- 网络协议安全的基本概念
- 典型的网络安全协议

学习目标：

（1）了解网络协议的安全问题；

（2）掌握网络协议安全的概念；

（3）熟悉一种典型网络安全协议（如 Kerberos，Open SSL 等协议）及其应用；

（4）了解提高网络协议安全性的措施。

NS-6 网络防护

最少学时：8 学时

知识点：

- 网络攻击与防护的概念
- 网络安全扫描技术
- 网络隔离技术

- 恶意代码防护
- 邮件安全防护
- 网络安全审计

学习目标：

（1）掌握网络攻击与防护的概念；

（2）了解 TCP/IP 的安全漏洞与威胁；

（3）熟悉安全扫描技术（端口扫描和漏洞扫描），能够使用常用安全扫描工具；

（4）掌握网络隔离的概念与原理；

（5）熟悉防火墙、网闸和 VLAN 技术等网络隔离技术的原理和方法；

（6）熟悉网络环境中的恶意代码防护技术，掌握一种恶意代码查杀工具的应用；

（7）了解邮件安全风险，掌握邮件安全检测的基本方法；

（8）了解网络安全审计技术。

NS-7 Web 安全

最少学时：6 学时

知识点：

- Web 安全威胁
- Web 安全防护技术

学习目标：

（1）了解 Web 安全威胁和防御方法；

（2）了解 HTTPS 协议；

（3）熟悉 Web 认证技术；

（4）熟悉网页过滤和防篡改的基本原理。

NS-8 无线网络安全（选修）

最少学时：12 学时

知识点：

- 无线网络的安全弱点
- 无线网络安全策略
- 无线网络安全协议
- 无线网络接入安全
- 移动通信网络安全

学习目标：

(1) 掌握无线网络安全的概念；
(2) 了解无线网络的安全弱点；
(3) 熟悉无线网络安全策略的制定和实施；
(4) 熟悉无线通信网络的数据加密、认证技术和授权技术；
(5) 了解无线网络安全协议；
(6) 了解无线接入网络安全问题与基本技术（如 WLAN 等）；
(7) 了解移动通信网络安全问题与基本技术（如 2G/3G/4G 等）；
(8) 熟悉一种智能移动终端的安全问题和安全机制。

5. ICS 信息内容安全(8+38 学时)

(1) ICS-1 信息内容安全概念
(2) ICS-2 网络数据的获取
(3) ICS-3 信息内容的分析与识别（选修）
(4) ICS-4 信息内容的管控（选修）
(5) ICS-5 多媒体信息隐藏（选修）
(6) ICS-6 隐私保护（选修）

信息内容安全是信息安全在法律、政治、道德层次上的要求。我们要求信息内容是安全的，就是要求信息内容在政治上是健康的，在法律上是符合国家法律法规的，在道德上是符合中华民族优良的道德规范的。信息

内容安全旨在获取数据，分析信息内容是否符合我国法律、政治、道德的要求，确保合法内容的安全，阻止非法内容的传播和利用。

目前学术界对信息内容安全的认识尚不一致。广义的信息内容安全既包括信息内容在政治、法律和道德方面的要求，也包括信息内容的保密、知识产权保护、信息隐藏、隐私保护等诸多方面。

信息隐藏技术是一种把一个秘密信息隐藏到另一载体中去，并使未授权者不易感知和获取这一个秘密信息的技术。信息隐藏技术可以分为隐蔽信道技术和多媒体信息隐藏技术。隐蔽信道技术利用各种隐蔽信道来实现秘密信息的隐藏和传输。多媒体信息隐藏以多媒体信号为载体，利用多媒体数据的数据冗余和人们的听视觉冗余来隐藏秘密信息。与信息隐藏对立的技术称为信息隐藏分析技术，研究如何攻击信息隐藏以获取所隐藏的秘密信息。信息隐藏不同于密码技术。密码技术把秘密信息编码成不被识别的密文，以达到信息保密的目的。而信息隐藏则是把秘密信息隐藏到另一载体中，以达到信息保密的目的。显然，密码技术和信息隐藏技术都是信息内容保护技术，但是两种技术各有不同的优缺点。

隐私是不愿意公开或不愿意告诉别人的个人信息。公民享有隐私权。世界上许多国家都颁布了相关的法律，保护公民的隐私权。但是随着社会的信息化，网络上的个人信息越来越多，危害公民隐私权、泄漏公民隐私的事件也越来越多。保护公民隐私权，除了采用法律保护之外，还必须采用技术手段进行保护。

在这里既考虑信息内容在政治、法律和道德方面的要求，也考虑信息隐藏和隐私保护等方面的要求。而且强调信息内容安全中的基本概念、基本理论和基本技术。

通过学习信息内容安全，学生将可以了解信息内容安全的威胁，掌握信息内容安全的基本概念、基本理论、基本技术和基本应用。对于本规范的方案二，在这里更强调了相关技术应用性知识单元，适当减少了部分知识单元中的理论性内容或适当降低了要求。

信息内容安全的知识领域包括：信息内容安全概念，网络数据的获取，信息内容的分析与识别（选修），信息内容的管控（选修），多媒体信息隐藏（选修），隐私保护（选修），共 6 个知识单元。

ICS-1 信息内容安全概念

最少学时：2 学时

知识点：

- 信息内容安全的概念
- 信息内容安全的威胁
- 确保信息内容安全的措施

学习目标：

（1）掌握信息内容安全的概念；

（2）了解信息内容安全的威胁；

（3）了解确保信息内容安全的技术措施与法律法规保障。

ICS-2 网络数据的获取

最少学时：6 学时

知识点：

- 网络数据获取的概念
- 网络数据的被动获取技术
- 网络数据的主动获取技术
- 网络协议还原技术

学习目标：

（1）掌握网络数据获取的概念；

（2）掌握常用的网络数据被动获取技术；

（3）熟悉常用的网络数据主动获取技术；

（4）掌握一种网络协议还原技术；

（5）了解网络数据获取技术的应用。

ICS-3 信息内容的分析与识别（选修）

最少学时：6 学时

知识点：

- 信息内容分析与识别的概念
- 基于文本的特征串匹配技术
- 文本分类技术
- 数据挖掘技术

学习目标：

（1）掌握信息内容识别的概念；

（2）掌握一种基于文本的特征串匹配技术（单模式匹配，多模式匹配等匹配算法）；

（3）熟悉一种常用的数据挖掘技术；

（4）了解信息内容识别技术的应用。

ICS-4 信息内容的管控（选修）

最少学时：6 学时

知识点：

- 信息内容安全管控的概念
- 基于网络地址的阻断技术
- 基于内容的阻断技术
- 信息内容管控的相关法律法规

学习目标：

（1）掌握信息内容安全管控的概念；

（2）掌握基于网络地址（IP 地址，域名）的阻断技术；

（3）了解基于内容的阻断技术；

（4）了解信息内容管控相关的主要法律法规；

（5）了解信息内容管控技术的应用。

ICS-5 多媒体信息隐藏（选修）

最少学时：18 学时

知识点：

- 信息隐藏的概念
- 多媒体信息隐藏的概念与基本技术
- 隐写的概念与基本技术
- 数字水印的概念与基本技术
- 数字指纹的概念与基本技术
- 数字权益管理

学习目标：

（1）掌握信息隐藏的概念；

（2）掌握多媒体信息隐藏的基本原理与技术；

（3）了解隐写的原理与基本技术；

（4）熟悉数字水印的基本原理与技术；

（5）了解数字指纹的基本原理与技术；

（6）熟悉数字权益管理的概念，了解常用数字权益管理技术。

ICS-6 隐私保护（选修）

最少学时：8 学时

知识点：

- 隐私和隐私保护的概念
- 社会信息化对公民隐私的威胁
- 隐私保护的基本原理
- 隐私保护技术（如匿名技术，磁盘加密技术，磁盘数据擦除技术等）
- 隐私保护的法律保障

学习目标：

（1）掌握隐私和隐私保护的概念；

（2）了解社会信息化对公民隐私的威胁；

（3）掌握隐私保护的基本原理；

（4）熟悉隐私保护技术的综合性特点，掌握一种隐私保护技术；

（5）了解我国隐私保护的法律法规。

3.5 信息安全专业规范实践能力体系

信息安全专业实践能力体系是信息安全专业毕业生应当具备的实践能力的结构与集合。

实践能力体系要用实践教学体系来覆盖，通过实践教学体系的实施来培养提高学生的实践能力。实践教学体系由多种实践教学环节组成。

3.5.1 实践能力体系的结构

与知识体系对应，实践能力体系由一些实践能力领域、实践能力单元和实践能力点组成。一个实践能力领域包含若干个实践能力单元，一个实践能力单元又包括若干个实践能力点。图 3-6 给出了实践能力体系的层次结构。

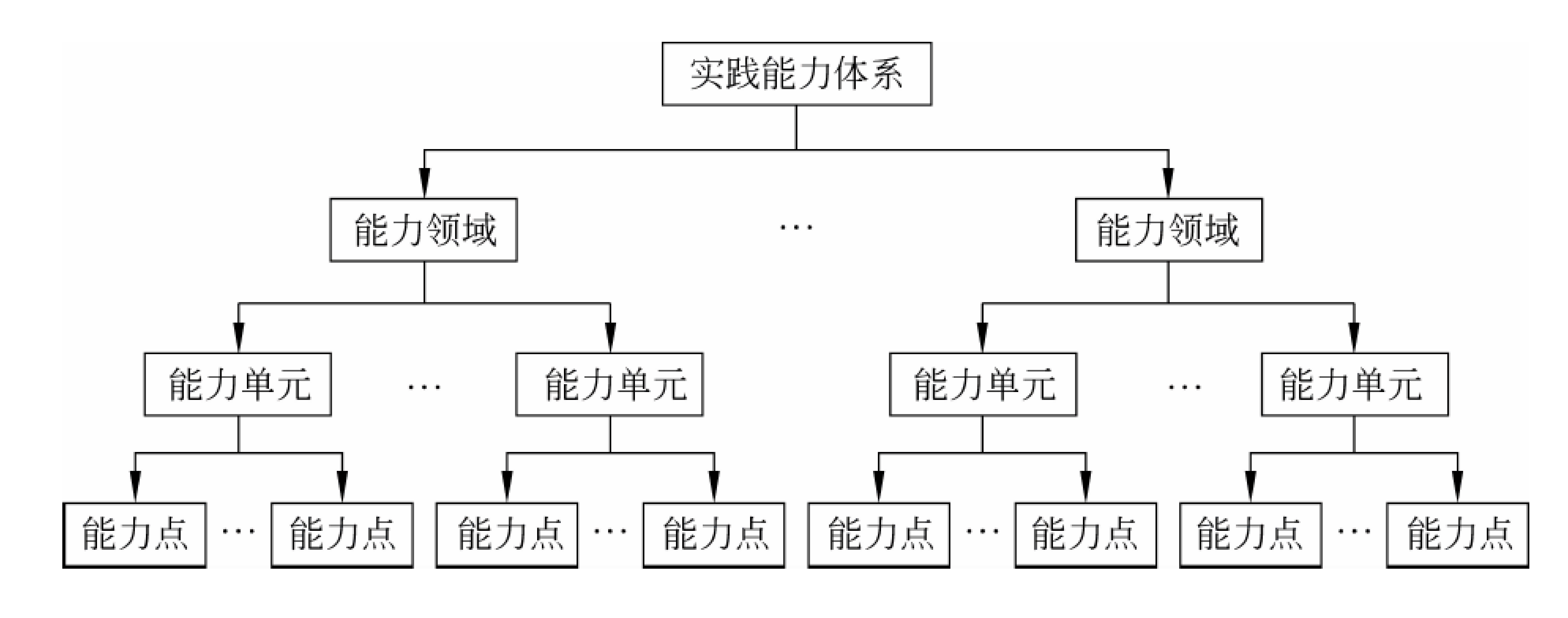


图 3-6　实践能力体系层次结构

图 3-7 给出了信息安全专业的实践能力体系的总体结构。它由软件系统实践能力领域、硬件系统实践能力领域、密码学实践能力领域、网络安

全实践能力领域、信息内容安全实践能力和创新实践能力领域组成。

图 3-7　实践能力体系结构

注意，在实践能力体系中，没有信息系统安全实践能力领域，这一点与知识体系不对应。这是因为，在这里设置了软件系统实践能力领域和硬件系统实践能力领域，我们把属于信息系统安全方面的一些实践能力单元和能力点，分别放置到软件系统实践能力领域和硬件系统实践能力领域中去了。

特别指出，严格地说，其中的软件系统实践能力领域和硬件系统实践能力领域的一部分内容是属于信息科学基础中的实践能力要求，可以不列在此实践能力体系中。但是，考虑到实践能力体系的完整性，我们还是把它们列在此处了。各个学校可以根据自己的信息安全专业所依托学科和办学特色，自己确定把哪些实践能力的教学活动安排到专业实践教学中，把哪些实践能力的教学活动安排到信息科学基础的实践教学中。合理的分配将会节省专业阶段的实践教学课时，以安排更多的选修内容，增强自己的办学特色和优势。

3.5.2　实践能力体系中的符号标识

在规范的实践能力体系中采用了以下的符号标识。

① 实践能力领域用其英文缩写来标识：

- 软件系统实践能力领域，用 SWSPA 标识。
- 硬件系统实践能力领域，用 HWSPA 标识。

• 密码学实践能力领域，用 CRYPTPA 标识。
• 网络安全实践能力领域，用 NSPA 标识。
• 信息内容安全实践能力领域，用 ICSPA 标识。
• 创新实践能力领域，用 CPA 标识。

② 实践能力领域下面的实践能力单元，采用“实践能力领域标识-序号”的方法来标识。如密码标准算法的实现与应用能力单元，用 CRYPTPA-1 标识。

3.5.3 实践能力体系方案一

1. SWSPA 软件系统实践能力(34+62 学时)

(1) SWSPA-1 编程基础实践能力
(2) SWSPA-2 网络编程实践能力
(3) SWSPA-3 基础软件实践能力
(4) SWSPA-4 小型应用软件实践能力（选修）
(5) SWSPA-5 恶意代码处理能力

软件系统是指由系统软件、支撑软件和应用软件组成的计算机软件系统，即是计算机系统中由软件组成的部分。它包括操作系统、语言处理系统、数据库系统、人机交互系统、应用软件系统等。

软件系统实践能力的目的是培养学生在软件系统方面的实际应用能力，包括软件编程的基本实践能力、基础软件的实际应用能力和小型软件的设计开发能力。通过软件系统实践能力的培养和锻炼，使学生不仅能够掌握软件的基本编程能力，掌握主流操作系统和数据库系统的实际应用能力，还能够针对小型软件工程项目，基本掌握软件工程管理、软件需求分析、软件设计、软件编码、软件测试、文档编写的基本能力。通过软件系统实践能力的培养和锻炼，使学生进一步理解和掌握软件开发模型、软件生命周期、软件过程等理论在软件项目开发过程中的指导意义和作用，培

养学生按照软件工程的原理、方法、技术、标准和规范进行软件开发的能力，培养学生的合作意识和团队精神，培养学生对技术文档的编写能力，从而使学生提高软件开发与应用的综合能力，提高软件项目的管理能力。

软件系统实践能力领域包括：编程基础实践能力、网络编程实践能力、基础软件实践能力、小型应用软件实践能力(选修)、恶意代码处理能力，共5个实践能力单元。

SWSPA-1 编程基础实践能力

最少学时：18＋24学时

能力点：

- SWSPA-1-1 汇编语言编程能力（选修）
- SWSPA-1-2 C语言编程能力
- SWSPA-1-3 Java语言编程能力（选修）

实践目标：

（1）能够阅读用汇编语言编写的程序，能使用一种汇编语言编写简单程序，并了解相应的调试方法；

（2）能使用主流的C语言开发工具进行小型软件的开发；

（3）能使用主流Java语言开发工具进行小型软件的开发。

SWSPA-2 网络编程实践能力

最少学时：12＋20学时

能力点：

- SWSPA-2-1 Web编程能力（选修）
- SWSPA-2-2 Socket编程能力
- SWSPA-2-3 网络安全编程能力（选修）

实践目标：

（1）掌握主流Web程序设计语言和框架，能够进行小型Web应用的开发；

（2）熟悉Socket编程机制与实现机理；

（3）掌握主流操作系统平台上的 Socket 开发方法，能够进行小型网络软件的开发；

（4）了解网络安全编程概念和基本方法。

SWSPA-3 基础软件实践能力

最少学时：2＋2 学时

能力点：

- 主流操作系统的安装及安全配置能力
- 主流数据库系统的安装及安全配置能力（选修）

实践目标：

（1）具有一种主流操作系统的安装能力；

（2）能够对一种主流操作系统进行用户设置和管理、目录和文件权限管理、网络服务安全管理、本地安全策略设定、策略审核和日志文件保护等系统安全配置；

（3）能够对一种主流数据库系统进行安装及安全配置。

SWSPA-4 小型应用软件实践能力（选修）

最少学时：12 学时

能力点：

- 需求分析能力
- 软件设计能力
- 软件编码能力
- 软件测试能力
- 文档编写能力

实践目标：

（1）具备小型应用软件的需求分析能力；

（2）具备小型应用软件的设计能力；

（3）具备软件的编码能力；

（4）具备软件测试的基本能力；

(5) 具备文档编写能力。

SWSPA-5 恶意代码处理能力

最少学时：2＋4 学时

能力点：

- 使用工具查杀恶意代码的能力
- 恶意代码分析能力(选修)
- 手工查杀恶意代码的能力(选修)

实践目标：

(1) 具有使用常见恶意代码查杀工具，查杀恶意代码(病毒、木马、蠕虫等)的能力；

(2) 具有简单恶意代码的分析能力；

(3) 具有手工查杀恶意代码(病毒、木马、蠕虫等)的能力与问题诊断处理能力。

2. HWSPA 硬件系统实践能力(22＋24 学时)

(1) HWSPA-1 模拟电路与数字电路应用能力

(2) HWSPA-2 可编程集成电路应用能力 (选修)

(3) HWSPA-3 嵌入式系统应用开发能力

(4) HWSPA-4PC 组配能力 (选修)

硬件是组成一切信息系统的物质基础，无论将来信息技术发展到多么高级的阶段，作为信息系统物质基础的硬件将永远发挥其重要的基础作用。因此，硬件系统实践能力成为信息安全专业学生的一种重要的实践能力。

通过硬件系统实践能力的培养和锻炼，学生可以在观察实物及动手实践的基础上对硬件系统有直观的认识，具有对模拟电路、数字电路、微处理器和嵌入式系统等基本硬件系统的分析、设计和制作能力，具备计算机的组配能力。

硬件系统实践能力领域主要包括：模拟电路与数字电路应用能力、可编程集成电路应用能力（选修）、嵌入式系统应用开发能力、PC组配能力（选修），共4个实践能力单元。

HWSPA-1 模拟电路与数字电路应用能力

最少学时：10＋10学时

能力点：

- 模拟电路应用能力（选修）
- 数字电路应用能力

实践目标：

（1）能够利用基本模拟电路进行简单应用的设计、分析和调试；

（2）能够利用基本数字电路进行简单应用的设计、分析和调试。

HWSPA-2 可编程集成电路应用能力（选修）

最少学时：10学时

能力点：

- 可编程器件的应用能力
- 硬件描述语言编程能力

实践目标：

（1）熟悉一种可编程器件（如CPLD或FPGA等）；

（2）熟悉利用可编程器件进行小型硬件部件的设计方法；

（3）掌握一种硬件描述语言（如VHDL或Verilog等），具有利用可编程器件进行小型应用部件的开发编程能力。

HWSPA-3 嵌入式系统应用开发能力

最少学时：12学时

能力点：

- 智能卡或USB-Key的应用及开发能力
- 基于主流嵌入式设备（如ARM或X86）的系统应用及开发

能力
- 智能移动终端的安全配置及应用开发能力

实践目标：

（1）了解智能卡或USB-Key的硬件结构、接口通信及其嵌入式操作系统；

（2）了解ARM或X86的硬件结构、接口通信及其嵌入式操作系统；

（3）具备下列能力之一：

① 基本的智能卡应用及开发能力；

② 基本的USB-Key应用及开发能力；

③ 基本的ARM嵌入式设备的应用开发能力；

④ 基本的X86嵌入式设备的应用开发能力；

⑤ 基本的智能移动终端的安全配置及应用开发能力。

HWSPA-4 PC组配能力（选修）

最少学时：4学时

能力点：

- PC组配能力
- PC硬件性能测试能力

实践目标：

（1）能够进行PC的组装；

（2）能够进行简单的PC故障定位。

3. CRYPTPA 密码学实践能力（8＋14学时）

（1）CRYPTPA-1 密码标准算法的软件实现与应用能力

（2）CRYPTPA-2 常用密码函数库及软件工具应用能力（选修）

密码技术是信息安全的关键技术之一，几乎所有的信息安全系统都应用到密码技术。密码学具有很深入的理论性，而密码学的应用又具有很强

的实践性。要想把密码学的知识应用到实际中去，必须具有密码学的实践应用能力。因此，密码学实践能力成为信息安全专业学生应当具备的实践能力的重要组成部分。

通过密码学实践能力的培养和锻炼，学生将能掌握密码标准算法的实现与应用能力，能够使用常用密码软件工具（如 PGP，Open SSL 等），进而具有一定的密码技术应用能力。

密码学实践能力领域主要包括：密码标准算法的实现与应用能力、常用密码函数库及软件工具应用能力(选修)，共两个实践能力单元。

CRYPTPA-1 密码标准算法的软件实现与应用能力

最少学时：8＋6 学时

能力点：

- 3DES 或 AES 或 SMS4 的软件实现能力
- 3DES 或 AES 或 SMS4 的硬件实现能力(选修)
- 3DES 或 AES 或 SMS4 实现的应用能力

实践目标：

（1）具有 3DES 或 AES 或 SMS4 的软件实现能力；

（2）具有 3DES 或 AES 或 SMS4 的硬件实现能力；

（3）具有文件加密系统（利用 3DES 或 AES 或 SMS4 密码）的开发能力。

CRYPTPA-2 常用密码函数库及软件工具应用能力(选修)

最少学时：8 学时

能力点：

- CryptoAPI 或 CDSA 或 JCE 的使用能力
- 常用密码应用软件（如 PGP，Open SSL 等）的应用能力

实践目标：

（1）熟悉 CryptoAPI 或 CDSA 或 JCE；

（2）具有 CryptoAPI 或 CDSA 或 JCE 的应用能力；

（3）具有一种密码软件工具（如 PGP 或 Open SSL 或其他）的应用能力。

4. NSPA 网络安全实践能力(28＋8 学时)

（1）NSPA-1 常用网络安全设备安装与配置能力

（2）NSPA-2 服务器环境搭建与安全配置能力（选修）

（3）NSPA-3 网络安全防护能力

（4）NSPA-4 小型网络安全整体解决方案设计能力

（5）NSPA-5 Web 安全实践能力

网络安全是信息安全的重要内容之一。网络安全的多数内容具有很强的技术性，若不进行实践，就不可能掌握这些知识，更不可能会实际应用。因此，网络安全实践能力是信息安全专业学生应当具备的重要实践能力。

通过网络安全实践能力的培养和锻炼，学生能够通过实例分析网络的安全威胁，具备常用网络安全工具的使用能力，熟悉常用网络设备的安全配置，具备小型网络安全解决方案的初步设计能力。

网络安全实践能力领域主要包括：常用网络安全设备安装与配置能力、服务器环境搭建与安全配置能力（选修）、网络安全防护能力、小型网络安全整体解决方案设计能力、Web 安全实践能力，共 5 个实践能力单元。

NSPA-1 常用网络安全设备安装与配置能力

最少学时：6 学时

能力点：

- 防火墙的应用能力
- 入侵检测系统（IDS）的应用能力
- 虚拟专用网络（VPN）的应用能力

实践目标：

（1）具备防火墙、IDS、VPN 的安装能力；

（2）具备防火墙、IDS、VPN 的基本安全配置能力。

NSPA-2 服务器环境搭建与安全配置能力（选修）

最少学时：4 学时

能力点：

- 服务器环境搭建能力
- 应用服务器的安全配置能力

实践目标：

（1）能够搭建 IIS＋.NET 环境并对其进行安全配置；

（2）能够搭建 Linux＋Apache＋Tomcat 环境并对其进行安全配置。

NSPA-3 网络安全防护能力

最少学时：8 学时

能力点：

- 典型扫描工具的使用能力
- 扫描报告的分析能力
- 网络攻击的检测与分析能力

实践目标：

（1）能够使用常用扫描软件工具进行安全扫描（端口扫描，漏洞扫描）；

（2）具有分析扫描报告的能力；

（3）熟悉防火墙、网闸和 VLAN 技术等网络隔离技术的应用；

（4）具有一种网络攻击的检测与分析能力（如恶意代码攻击）。

NSPA-4 小型网络安全整体解决方案设计能力

最少学时：8＋2 学时

能力点：

- 网络安全需求分析能力

- 网络安全策略制定能力
- 网络安全解决方案设计能力
- PKI 技术的应用能力（选修）

实践目标：

（1）能够分析网络环境下的安全威胁；

（2）能够进行安全需求分析；

（3）能够制定安全策略；

（4）能够针对安全需求设计出可行的小型网络安全解决方案；

（5）了解 PKI 技术的应用方法。

NSPA-5 Web 安全实践能力

最少学时：6＋2 学时

能力点：

- Web 服务器安全配置能力
- 网页防篡改技术的实现能力
- 单点登录技术的实现能力（选修）
- Web 攻击的检测与分析能力

实践目标：

（1）能够对一种 Web 服务器进行安全配置；

（2）能够应用一种网页防篡改技术；

（3）熟悉一种单点登录技术的实现方法；

（4）具有对典型 Web 攻击的检测与分析能力。

5. ICSPA 信息内容安全实践能力（4＋20 学时）

（1）ICSPA-1 网络数据获取能力

（2）ICSPA-2 信息内容的分析与识别能力（选修）

（3）ICSPA-3 信息内容的管控能力（选修）

（4）ICSPA-4 多媒体信息隐藏实践能力（选修）

（5）ICSPA-5 隐私保护实践能力（选修）

信息内容安全是信息安全在政治、法律、道德层次上的要求。我们要求信息内容是安全的，就是要求信息内容在政治上是健康的，在法律上是符合国家法律法规的，在道德上是符合中华民族优良的道德规范的。

通过信息内容安全实践能力的培养和锻炼，学生能够通过实例了解信息内容安全的威胁，掌握信息内容的获取、分析识别和管控能力，具有常用信息内容安全工具的使用能力；掌握多媒体信息隐藏和隐私保护的一些基本能力。

信息内容安全实践能力领域主要包括：网络数据的获取能力、信息内容的分析与识别能力（选修）、信息内容的管控能力（选修）、多媒体信息隐藏实践能力（选修）、隐私保护实践能力（选修），共 5 个实践能力单元。

ICSPA-1 网络数据获取能力

最少学时：4 学时

能力点：

- 网络数据的被动获取能力
- 网络数据的主动获取能力

实践目标：

（1）能够通过编程实现网络数据的被动获取；

（2）能够使用常用网络数据获取工具获取网络数据（主动获取或被动获取）。

ICSPA-2 信息内容的分析与识别能力（选修）

最少学时：4 学时

能力点：

- 信息内容的提取能力
- 信息内容的分析与识别能力

实践目标：

（1）具有应用基于文本特征串匹配技术（单模式匹配，多模式匹配等）进行信息内容的分析与识别的能力；

（2）能够使用常用信息内容分析与识别工具。

ICSPA-3 信息内容的管控能力（选修）

最少学时：4 学时

能力点：

- 基于网络地址的信息内容管控能力
- 基于内容的信息内容管控能力

实践目标：

（1）具有基于网络地址（IP 地址和域名）对不良信息进行阻断的能力；

（2）能够使用常用的网络不良信息阻断工具。

ICSPA-4 多媒体信息隐藏实践能力（选修）

最少学时：6 学时

能力点：

- 数字水印的软件实现能力
- 数字指纹的软件实现能力
- 数字权益管理工具的应用能力

实践目标：

（1）具有常用数字水印算法的软件实现能力；

（2）初步具有数字指纹的软件实现能力；

（3）具有一种数字权益管理工具的使用能力。

ICSPA-5 隐私保护实践能力（选修）

最少学时：6 学时

能力点：

- 隐私保护状况的调查与分析能力
- 磁盘加密能力
- 磁盘数据擦除能力

实践目标：

（1）能够对隐私状况进行调查，并写出调查分析报告；

（2）针对调查分析结果，能够提出相应的技术增强基本方案；

（3）能够利用工具实现磁盘加密和磁盘数据擦除。

6. CPA 创新实践能力（0＋20 学时）（选修）

创新型实验是大学生本科阶段重要的一环，培养学生分析问题、解决问题的基本能力以及知识综合运用能力，包括资料检索、试验设计、方案比较、实验实施、数据分析和实验总结等环节，提高学生的创新意识、综合实践能力和团队合作精神。

在教师指导下完成一个创新型实验，要求：

① 自主命题

② 自主设计

③ 自主实现

④ 自主分析

⑤ 实验设计有一定新意，或实验结果有一定应用价值，且实验至少要覆盖三个能力单元

最少学时： 20 学时

能力点：

- 创新能力
- 综合实践能力
- 团队合作能力

实践目标：

（1）具有文献资料检索和阅读能力；

（2）具有实验设计能力；

（3）具有实施实验的能力；

（4）具有技术文档的编写能力；

（5）具有分析实验数据和实验总结的能力。

3.5.4　实践能力体系方案二

1. SWSPA 软件系统实践能力(50＋46 学时)

（1）SWSPA-1 编程基础实践能力

（2）SWSPA-2 网络编程实践能力

（3）SWSPA-3 基础软件实践能力

（4）SWSPA-4 小型应用软件实践能力（选修）

（5）SWSPA-5 恶意代码处理能力

软件系统是指由系统软件、支撑软件和应用软件组成的计算机软件系统，即是计算机系统中由软件组成的部分。它包括操作系统、语言处理系统、数据库系统、人机交互系统、应用软件系统等。

软件系统实践能力的目的是培养学生在软件系统方面的实际应用能力，包括软件编程的基本实践能力、基础软件的实际应用能力和小型软件的设计开发能力。通过软件系统实践能力的培养和锻炼，使学生不仅能够掌握软件的基本编程能力，掌握主流操作系统和数据库系统的实际应用能力，还能够针对小型软件工程项目，基本掌握软件工程管理、软件需求分析、软件设计、软件编码、软件测试、文档编写的基本能力。通过软件系统实践能力的培养和锻炼，帮助学生进一步理解和掌握软件开发模型、软件生命周期、软件过程等理论在软件项目开发过程中的指导意义和作用，培养学生按照软件工程的原理、方法、技术、标准和规范进行软件开发的

能力，培养学生的合作意识和团队精神，培养学生对技术文档的编写能力，从而使学生提高软件开发与应用的综合能力，提高软件项目的管理能力。

软件系统实践能力领域包括：编程基础实践能力、网络编程实践能力、基础软件实践能力、小型应用软件实践能力（选修）、恶意代码处理能力，共5个实践能力单元。

SWSPA-1 编程基础实践能力

最少学时：30＋12学时

能力点：

- SWSPA-1-1　汇编语言编程能力（选修）
- SWSPA-1-2　C语言编程能力
- SWSPA-1-3　Java语言编程能力

实践目标：

（1）能够阅读汇编语言编写的程序，能够使用一种汇编语言编写简单程序，并了解相应的调试方法；

（2）能够使用主流的C语言开发工具，进行小型软件的开发；

（3）能够使用主流Java语言开发工具，进行小型软件开发。

SWSPA-2 网络编程实践能力

最少学时：12＋20学时

能力点：

- SWSPA-2-1　Web编程能力（选修）
- SWSPA-2-2　Socket编程能力
- SWSPA-2-3　网络安全编程能力（选修）

实践目标：

（1）掌握主流Web程序设计语言和框架，能够进行小型Web应用的开发；

（2）熟悉Socket编程机制与实现机理；

(3) 掌握主流操作系统平台上的 Socket 开发方法，能够进行小型网络软件的开发；

(4) 了解网络安全编程概念和基本方法。

SWSPA-3 基础软件实践能力

最少学时：2+2 学时

能力点：

- 主流操作系统的安装及安全配置能力
- 主流数据库系统的安装及安全配置能力（选修）

实践目标：

(1) 具有一种主流操作系统的安装能力；

(2) 能够对一种主流操作系统进行用户设置和管理、目录和文件权限管理、网络服务安全管理、本地安全策略设定、策略审核和日志文件保护等系统安全配置；

(3) 能够对一种主流数据库系统进行安装及安全配置。

SWSPA-4 小型应用软件实践能力（选修）

最少学时：12 学时

能力点：

- 需求分析能力
- 软件设计能力
- 软件编码能力
- 软件测试能力
- 文档编写能力

实践目标：

(1) 具备小型应用软件的需求分析能力；

(2) 具备小型应用软件的设计能力；

(3) 具备软件的编码能力；

(4) 具备软件测试的基本能力；

（5）具备文档编写的能力。

SWSPA-5 恶意代码处理能力

最少学时：6 学时

能力点：

- 使用工具查杀恶意代码的能力
- 恶意代码分析能力
- 手工查杀恶意代码的能力

实践目标：

（1）具有使用常见恶意代码查杀工具，查杀恶意代码（病毒、木马、蠕虫等）的能力；

（2）具有捕获和分析恶意代码样本的能力；

（3）具有手工查杀恶意代码（病毒、木马、蠕虫等）的能力与问题诊断处理能力。

2. HWSPA 硬件系统实践能力（22＋24 学时）

（1）HWSPA-1 模拟电路与数字电路应用能力

（2）HWSPA-2 可编程集成电路应用能力（选修）

（3）HWSPA-3 嵌入式系统应用开发能力

（4）HWSPA-4 PC 组配能力（选修）

硬件是组成一切信息系统的物质基础，无论将来信息技术发展到多么高级的阶段，作为信息系统物质基础的硬件将永远发挥其重要的基础作用。因此，硬件系统实践能力成为信息安全专业学生的一种重要的实践能力。

通过硬件系统实践能力的培养和锻炼，学生可以在观察实物及动手实践的基础上对硬件系统有直观的认识，具有对模拟电路、数字电路、微处理器、嵌入式系统等基本硬件系统的分析、设计和制作能力，具备计算机的组配能力。

硬件系统实践能力领域主要包括：模拟电路与数字电路应用能力、可编程集成电路应用能力（选修）、嵌入式系统应用开发能力、PC 组配能力（选修），共 4 个实践能力单元。

HWSPA-1 模拟电路与数字电路应用能力

最少学时：10＋10 学时

能力点：

- 模拟电路应用能力（选修）
- 数字电路应用能力

实践目标：

（1）能够利用基本模拟电路进行简单应用的设计、分析和调试；

（2）能够利用基本数字电路进行简单应用的设计、分析和调试。

HWSPA-2 可编程集成电路应用能力（选修）

最少学时：10 学时

能力点：

- 可编程器件的应用能力
- 硬件描述语言编程能力

实践目标：

（1）熟悉一种可编程器件（如 CPLD 或 FPGA 等）；

（2）熟悉利用可编程器件进行小型硬件部件的设计方法；

（3）掌握一种硬件描述语言（如 VHDL 或 Verilog 等），具有利用可编程器件进行小型应用部件的开发编程能力。

HWSPA-3 嵌入式系统应用开发能力

最少学时：12 学时

能力点：

- 智能卡或 USB-Key 的应用及开发能力
- 基于主流嵌入式设备（如 ARM 或 X86）的系统应用及开发

能力

- 智能移动终端的安全配置及应用开发能力

实践目标：

(1) 了解智能卡或USB-Key的硬件结构、接口通信及其嵌入式操作系统；

(2) 了解ARM或X86的硬件结构、接口通信及其嵌入式操作系统；

(3) 具备下列能力之一：

① 基本的智能卡应用及开发能力；

② 基本的USB-Key应用及开发能力；

③ 基本的ARM嵌入式设备的应用开发能力；

④ 基本的X86嵌入式设备的应用开发能力；

⑤ 基本的智能移动终端的安全配置及应用开发能力。

HWSPA-4 PC组配能力(选修)

最少学时： 4学时

能力点：

- PC组配能力
- PC硬件性能测试能力

实践目标：

(1) 能够进行PC的安装组配；

(2) 能够进行简单的PC故障定位。

3. CRYPTPA 密码学实践能力(16+6学时)

(1) CRYPTPA-1 密码标准算法的软件实现与应用能力

(2) CRYPTPA-2 常用密码函数库及软件工具应用能力

密码技术是信息安全的关键技术之一，几乎所有的信息安全系统都应用到密码技术。密码学具有很深入的理论性，而密码学的应用又具有很强

的实践性。要想把密码学的知识应用到实际中去，必须具有密码学的实践应用能力。因此，密码学实践能力成为信息安全专业学生应当具备的实践能力的重要组成部分。

通过密码学实践能力的培养和锻炼，学生将能掌握密码标准算法的实现与应用能力，能够使用常用密码软件工具（如 PGP，Open SSL 等），进而具有一定的密码技术应用能力。

密码学实践能力领域主要包括：密码标准算法的实现与应用能力、常用密码函数库及软件工具应用能力（选修），共两个实践能力单元。

CRYPTPA-1 密码标准算法的软件实现与应用能力

最少学时：8＋6 学时

能力点：

- 3DES 或 AES 或 SMS4 的软件实现能力
- 3DES 或 AES 或 SMS4 的硬件实现能力（选修）
- 3DES 或 AES 或 SMS4 实现的应用能力

实践目标：

（1）具有 3DES 或 AES 或 SMS4 的软件实现能力；

（2）具有 3DES 或 AES 或 SMS4 的硬件实现能力；

（3）具有文件加密系统（利用 3DES 或 AES 或 SMS4 密码）的开发能力。

CRYPTPA-2 常用密码函数库及软件工具应用能力

最少学时：8 学时

能力点：

- CryptoAPI 或 CDSA 或 JCE 的使用能力
- 常用密码应用软件（如 PGP，Open SSL 等）的应用能力

实践目标：

（1）熟悉 CryptoAPI 或 CDSA 或 JCE；

（2）具有 CryptoAPI 或 CDSA 或 JCE 的应用能力；

(3) 具有一种密码软件工具 (如 PGP, Open SSL 或其他) 的应用能力。

4. NSPA 网络安全实践能力 (32+10 学时)

(1) NSPA-1 常用网络安全设备安装与配置能力

(2) NSPA-2 服务器环境搭建与安全配置能力

(3) NSPA-3 网络安全防护能力

(4) NSPA-4 小型网络安全整体解决方案设计能力

(5) NSPA-5 Web 安全实践能力

网络安全是信息安全的重要内容之一。网络安全的多数内容具有很强的技术性，若不进行实践，就不可能掌握这些知识，更不可能会实际应用。因此，网络安全实践能力是信息安全专业学生应当具备的重要实践能力。

通过网络安全实践能力的培养的锻炼，学生能够通过实例分析网络的安全威胁，具备常用网络安全工具的使用能力，熟悉常用网络设备的安全配置，具备小型网络安全解决方案的初步设计能力。

网络安全实践能力领域主要包括：常用网络安全设备安装与配置能力、服务器环境搭建与安全配置能力、网络安全防护能力、小型网络安全整体解决方案设计能力、Web 安全实践能力，共 5 个实践能力单元。

NSPA-1 常用网络安全设备安装与配置能力

最少学时： 6 学时

能力点：

- 防火墙的应用能力
- 入侵检测系统 (IDS) 的应用能力
- 虚拟专用网络 (VPN) 的应用能力

实践目标：

(1) 具备防火墙、IDS、VPN 的安装能力；

（2）具备防火墙、IDS、VPN 的基本安全配置能力。

NSPA-2 服务器环境搭建与安全配置能力

最少学时：4 学时

能力点：

- 服务器环境搭建能力
- 应用服务器的安全配置能力

实践目标：

（1）能够搭建 IIS+.NET 环境并对其进行安全配置；

（2）能够搭建 Linux+Apache+Tomcat 环境并对其进行安全配置。

NSPA-3 网络安全防护能力

最少学时：8 学时

能力点：

- 典型扫描工具的使用能力
- 扫描报告的分析能力
- 网络攻击的检测与分析能力

实践目标：

（1）能够使用常用扫描软件工具进行安全扫描（端口扫描，主机扫描，漏洞扫描）；

（2）具有分析扫描报告的能力；

（3）熟悉防火墙、网闸和 VLAN 技术等网络隔离技术的应用；

（4）具有一种网络攻击的检测与分析能力（如恶意代码攻击等）。

NSPA-4 小型网络安全整体解决方案设计能力

最少学时：8+8 学时

能力点：

- 网络安全需求分析能力

- 网络安全策略制定能力
- 网络安全解决方案设计能力
- PKI 技术的应用能力（选修）
- 产品选型能力（选修）
- 网络安全解决方案实施能力（选修）

实践目标：

（1）能够分析网络环境下的安全威胁；
（2）能够分析应对威胁的安全需求；
（3）掌握网络安全域的划分原则和方法；
（4）能够针对安全需求设计出可行的网络安全解决方案；
（5）能够根据实际情况选择合适的安全产品；
（6）能够制定可行的实施方案；
（7）了解 PKI 技术的应用方法。

NSPA-5 Web 安全实践能力

最少学时：6＋2 学时

能力点：

- Web 服务器安全配置能力
- 网页防篡改技术的实现能力
- 单点登录技术的实现能力（选修）
- Web 攻击的检测与分析能力

实践目标：

（1）能够对一种 Web 服务器进行安全配置；
（2）能够应用一种网页防篡改技术；
（3）熟悉一种单点登录技术的实现方法；
（4）具有对典型 Web 攻击的检测与分析能力。

5. ICSPA 信息内容安全实践能力（4＋20 学时）

（1）ICSPA-1 网络数据获取能力

（2）ICSPA-2 信息内容的分析与识别能力（选修）

（3）ICSPA-3 信息内容的管控能力（选修）

（4）ICSPA-4 多媒体信息隐藏实践能力（选修）

（5）ICSPA-5 隐私保护实践能力（选修）

信息内容安全是信息安全在政治、法律、道德层次上的要求。我们要求信息内容是安全的，就是要求信息内容在政治上是健康的，在法律上是符合国家法律法规的，在道德上是符合中华民族优良的道德规范的。

通过信息内容安全实践能力的培养和锻炼，学生能够通过实例了解信息内容安全的威胁，掌握信息内容的获取、分析识别和管控能力，具有常用信息内容安全工具的使用能力；掌握多媒体信息隐藏和隐私保护的一些基本能力。

信息内容安全实践能力领域主要包括：网络数据的获取能力、信息内容的分析与识别能力（选修）、信息内容的管控能力（选修）、多媒体信息隐藏实践能力（选修）和隐私保护实践能力（选修），共 5 个实践能力单元。

ICSPA-1 网络数据获取能力

最少学时：4 学时

能力点：

- 网络数据的被动获取能力
- 网络数据的主动获取能力

实践目标：

（1）能够通过编程实现网络数据的被动获取；

（2）能够使用常用网络数据获取（主动和被动）工具获取网络数据。

ICSPA-2 信息内容的分析与识别能力（选修）

最少学时：4 学时

能力点：

- 信息内容的提取能力
- 信息内容的分析与识别能力

实践目标：

（1）具有应用基于文本特征串匹配技术（单模式匹配，多模式匹配等）进行信息内容的分析与识别的能力；

（2）能够使用常用信息内容分析与识别工具。

ICSPA-3 信息内容的管控能力（选修）

最少学时：4 学时

能力点：

- 基于网络地址的信息内容管控能力
- 基于内容的信息内容管控能力

实践目标：

（1）具有基于网络地址（IP 地址和域名）对不良信息进行阻断的能力；

（2）能够使用常用的网络不良信息阻断工具。

ICSPA-4 多媒体信息隐藏实践能力（选修）

最少学时：6 学时

能力点：

- 数字水印的软件实现能力
- 数字指纹的软件实现能力
- 数字权益管理工具的应用能力

实践目标：

（1）具有常用数字水印算法的软件实现能力；

（2）初步具有数字指纹的软件实现能力；

（3）具有一种数字权益管理工具的使用能力。

ICSPA-5 隐私保护实践能力（选修）

最少学时：6 学时

能力点：

- 隐私保护状况的调查与分析能力
- 磁盘加密能力
- 磁盘数据擦除能力

实践目标：

（1）能够对隐私状况进行调查，并写出调查分析报告；

（2）针对调查分析结果，能够提出相应的技术增强基本方案；

（3）能够利用工具实现磁盘加密和磁盘数据擦除。

6. CPA 创新实践能力（0＋20 学时）（选修）

创新型实验是大学生本科阶段最重要的一环，培养学生分析问题、解决问题的基本能力以及知识综合运用能力，包括资料搜索、试验设计、试验完成、团队合作、方案比较和实验总结等环节，提高学生的创新意识和综合实践能力。

在教师指导下完成一个创新型实验，要求：

① 自主命题

② 自主设计

③ 自主实现

④ 自主分析

⑤ 实验设计有一定新意，或实验结果有一定应用价值，且实验至少要覆盖三个能力单元

最少学时：20 学时

能力点：

- 创新能力
- 综合实践能力

- 团队合作能力

实践目标：

（1）具有文献资料检索和阅读能力；

（2）具有实验设计能力；

（3）具有完成实验的能力；

（4）具有技术文档的编写能力；

（5）具有分析实验数据和实验总结的能力。

3.6 信息安全专业知识体系和实践能力体系两套方案的比较

知识体系和实践能力体系两套方案的比较如表 3-1 和表 3-2 所示。

表 3-1 知识体系两套方案比较

	知识领域	信息安全基础	密码学	信息系统安全	网络安全	信息内容安全	最少课时合计
方案一	最少必修学时	52	52	60	44	8	216
	最少选修学时	82	0	36	12	38	168
方案二	最少必修学时	28	34	60	44	8	174
	最少选修学时	0	0	38	12	38	88

从表 3-1 中可以看出：

（1）从两个方案的总学时数方面看：方案一的最少必修学时数合计为 216 学时，而方案二的最少必修学时数合计为 174 学时，方案二比方案一少 42 个学时。方案一的最少选修学时数合计为 168 学时，而方案二的最少选

修学时数合计为 88 学时，方案二比方案一少 80 个学时。这说明方案二在知识体系方面的要求比方案一稍低一些。

（2）从知识领域的学时数方面看：

① 方案一与方案二在网络安全和信息内容安全知识领域的学时要求是一致的，在信息系统安全知识领域的学时要求也是基本一致的。

② 方案一与方案二的学时数差异主要体现在信息安全基础和密码学两个知识领域中。

③ 方案二在信息安全基础知识领域中无论是必修最少学时还是选修最少学时数都比方案一要少，而这种差异主要是在方案二中对信息安全数学基础要求较低造成的。这说明在方案二中对信息安全基础知识领域的要求较低。

④ 方案二在密码学知识领域中最少必修学时数也比方案一要少，这说明在方案二中对密码学知识领域的要求较低。

表 3-2　实践能力体系两套方案比较

	实践能力领域	软件系统实践能力	硬件系统实践能力	密码学实践能力	网络安全实践能力	信息内容安全实践能力	创新实践能力	最少课时合计
方案一	最少必修学时	34	22	8	28	4	0	96
	最少选修学时	62	24	14	8	20	20	148
方案二	最少必修学时	50	22	16	32	4	0	124
	最少选修学时	46	24	6	10	20	20	126

从表 3-2 中可以看出：

（1）从两个方案的总学时数方面看：方案一的最少必修学时数合计为

96学时，而方案二的最少必修学时数合计为124学时，方案二比方案一多28个学时。方案一的最少选修学时数合计为148学时，而方案二的最少选修学时数合计为126学时，方案二比方案一少22个学时。两者相差学时数的主要部分在方案一中是选修，而在方案二中变成必修。这说明方案二在实践能力体系方面的要求比方案一稍高。

(2) 从实践能力领域的学时数方面看：

① 方案一与方案二在硬件系统、信息内容安全和创新实践能力领域的学时数要求是一致的。

② 方案一与方案二的学时数差异主要体现在软件系统、密码学和网络安全三个实践能力领域中。

③ 方案二在软件系统实践能力领域中的最少必修学时是50，而方案一在软件系统实践能力领域中的最少必修学时是34，方案二比方案一多16学时。方案二在软件系统实践能力领域中的最少选修学时是46，而方案一在软件系统实践能力领域中的最少选修学时是62，方案二比方案一少16学时。两者相差的这16个学时恰好在方案一中是选修，而在方案二中变成必修。这说明在方案二中对软件系统实践能力领域的要求比方案一稍高。

④ 方案二在密码学实践能力领域中的最少必修学时是16，而方案一在密码学实践能力领域中的最少必修学时是8，方案二比方案一多8学时。方案二在密码学实践能力领域中的最少选修学时是6，而方案一在密码学实践能力领域中的最少选修学时是14，方案二比方案一少8学时。两者相差的这8个学时恰好在方案一中是选修，而在方案二中变成必修。这说明在方案二中对密码学实践能力领域的要求比方案一稍高。

⑤ 方案二在网络安全实践能力领域中的最少必修学时是32，而方案一在网络安全实践能力领域中的最少必修学时是28，方案二比方案一多4学时。方案二在网络安全实践能力领域中的最少选修学时是10，而方案一在网络安全实践能力领域中的最少选修学时是8，方案二比方案一多2学时。无论是最少必修学时还是最少选修学时，方案二都比方案一多。这说明在

方案二中对网络安全实践能力领域的要求比方案一稍高。

综合上面的比较，可知：

（1）两个方案总体上是有一定差异的，但是差异并不太大。

（2）这种差异不仅体现在最少学时数方面，还体现在对知识和实践能力的学习目标要求方面。这里主要比较了两个方案的学时数差异，没有比较学习目标要求方面的差异。希望学校在选择自己的方案时，能在学时数和学习目标要求两个方面进行仔细比较。

（3）方案一在知识的要求方面比方案二稍高。

（4）方案二在实践能力的要求方面比方案一稍高。

据此，每个学校可以自主地选择适合自己的一个方案，并且还可以自主更换。进一步在必修知识单元和必修实践能力单元之外增加自己的特色内容，并合理地确定自己的选修知识单元和选修实践能力单元，这样就一定可以办出自己的专业特色。

3.7　信息安全专业规范课程体系

规范的知识体系要用课程体系来覆盖，通过课程教学传授给学生。

3.7.1　课程体系设置原则

（1）知识体系用课程体系来覆盖：每一个必修知识点都必须被覆盖，不准遗漏。

（2）重要的知识点允许有一定的重复，一般地，重复度可为3左右。

（3）课程体系对知识体系的覆盖可以有多种方法，因此就可以有不同的课程体系方案。本规范给出一种课程体系举例，供大家参考。各学校完全可以设计自己的课程体系。

（4）依据知识点的关联原则，在组成课程体系时，尽量将密切相关的知识点放在一门课中。

（5）在组成课程体系时，要注意知识点之间的前驱与后继关系。要根据知识点之间的前驱与后继关系安排课程的前后顺序。

3.7.2 知识体系方案一的课程体系举例

知识体系方案一的课程体系举例如表 3-3 和表 3-4 所示。

表 3-3 知识体系方案一的课程与知识单元的涵盖关系

知识单元名称	知识单元编号	课程与编号								
		1	2	3	4	5	6	7	8	9
		信息安全导论 必修	信息安全数学基础 必修	密码学 必修	网络安全 必修	软件安全 必修	信息系统安全 必修	电子商务与电子政务安全 选修	信息隐藏 选修	信息内容安全 选修
信息安全概念	ISB-1	√		√	√		√			√
数论	ISB-2-1		√							
代数结构	ISB-2-2		√							
组合数学（选修）	ISB-2-3		√							
逻辑学（选修）	ISB-2-4		√							
信息论（选修）	ISB-2-5		√							
编码学（选修）	ISB-2-6		√							
计算复杂性（选修）	ISB-2-7		√							
信息安全法律基础	ISB-3	√						√		√
信息安全管理基础	ISB-4	√						√		√
信息系统安全概念	ISS-1	√					√			
信息系统设备安全	ISS-2						√			

续表

知识单元名称	知识单元编号	课程与编号								
		1	2	3	4	5	6	7	8	9
		信息安全导论 必修	信息安全数学基础 必修	密码学 必修	网络安全 必修	软件安全 必修	信息系统安全 必修	电子商务与电子政务安全 选修	信息隐藏 选修	信息内容安全 选修
信息系统可靠性技术	ISS-3						√			
访问控制	ISS-4				√		√			
操作系统安全	ISS-5						√			
数据库安全	ISS-6						√			
软件安全	ISS-7	√				√	√			
电子商务安全(选修)	ISS-8	√						√		
电子政务安全(选修)	ISS-9	√						√		
数字取证技术(选修)	ISS-10									√
嵌入式系统安全	ISS-11						√			
密码学概念	CRYPT-1	√	√	√					√	
分组密码	CRYPT-2			√						
流密码	CRYPT-3			√						
Hash 函数	CRYPT-4			√						
公钥密码	CRYPT-5			√						
密码协议	CRYPT-6			√	√					
数字签名	CRYPT-7			√						
认证	CRYPT-8			√	√					

续表

知识单元名称	知识单元编号	课程与编号								
		1	2	3	4	5	6	7	8	9
		信息安全导论 必修	信息安全数学基础 必修	密码学 必修	网络安全 必修	软件安全 必修	信息系统安全 必修	电子商务与电子政务安全 选修	信息隐藏 选修	信息内容安全 选修
密钥管理	CRYPT-9			√						
网络安全概念	NS-1	√			√	√				
防火墙	NS-2				√					
入侵检测系统	NS-3				√					
虚拟专用网	NS-4				√					
网络安全协议	NS-5				√					
网络防护	NS-6				√	√				
Web 安全	NS-7				√			√		
无线网络安全(选修)	NS-8				√					
信息内容安全概念	ICS-1	√			√				√	√
网络数据的获取	ICS-2				√					√
信息内容的分析与识别(选修)	ICS-3									√
信息内容的管控(选修)	ICS-4									√
多媒体信息隐藏(选修)	ICS-5								√	√
隐私保护(选修)	ICS-6	√			√				√	√

表 3-4　知识体系方案一的信息安全专业课程举例

序号	课程名称		必修知识单元	选修知识单元
1	基础类课程	信息安全导论	ISB-1,ISB-3,ISB-4,ISS-1,ISS-7,CRYPT-1,NS-1,ICS-1	ISS-8 ISS-9 ICS-6
2		信息安全数学基础	ISB-2-1,ISB-2-2,CRYPT-1	ISB-2-3 ISB-2-4 ISB-2-5 ISB-2-6 ISB-2-7
3	专业类课程	密码学	ISB-1,CRYPT-1,CRYPT-2,CRYPT-3,CRYPT-4,CRYPT-5,CRYPT-6,CRYPT-7,CRYPT-8,CRYPT-9	
4		网络安全	ISB-1,ISS-4,CRYPT-6,CRYPT-8,NS-1,NS-2,NS-3,NS-4,NS-5,NS-6,NS-7,ICS-2	NS-8 ICS-6
5		软件安全	ISS-7, NS-1,NS-6	
6		信息系统安全	ISB-1,ISS-1,ISS-2,ISS-3,ISS-4,ISS-5,ISS-6,ISS-7,ISS-11	
7	应用类课程	电子商务与电子政务安全(选修)	ISB-3,ISB-4,NS-7	ISS-8 ISS-9
8		信息隐藏(选修)	CRYPT-1,ICS-1	ICS-5 ICS-6
9		信息内容安全(选修)	ISB-1,ISB-3,ISB-4,ICS-1,ICS-2	ICS-3 ICS-4 ICS-5 ICS-6 ISS-10

3.7.3 知识体系方案二的课程体系举例

知识体系方案二的课程体系举例如表 3-5 和表 3-6 所示。

表 3-5 知识体系方案二的课程与知识单元的涵盖关系

知识单元名称	知识单元编号	课程与编号								
		1	2	3	4	5	6	7	8	9
		信息安全导论 必修	应用密码学 必修	网络安全 必修	软件安全 必修	信息系统安全 必修	电子商务与电子政务安全 选修	信息犯罪与取证技术 选修	信息隐藏 选修	信息内容安全 选修
信息安全概念	ISB-1	√	√	√		√				√
信息安全数学基础	ISB-2		√							
信息安全法律基础	ISB-3	√					√	√		√
信息安全管理基础	ISB-4	√					√	√		√
信息系统安全概念	ISS-1	√				√				
信息系统设备安全	ISS-2					√				
信息系统可靠性技术	ISS-3					√				
访问控制	ISS-4			√		√				
操作系统安全	ISS-5					√		√		
数据库安全	ISS-6					√		√		
软件安全	ISS-7	√			√	√				
电子商务安全(选修)	ISS-8	√					√			
电子政务安全(选修)	ISS-9	√					√			
数字取证技术(选修)	ISS-10							√		√

续表

知识单元名称	知识单元编号	课程与编号								
		1	2	3	4	5	6	7	8	9
		信息安全导论 必修	应用密码学 必修	网络安全 必修	软件安全 必修	信息系统安全 必修	电子商务与电子政务安全 选修	信息犯罪与取证技术 选修	信息隐藏 选修	信息内容安全 选修
嵌入式系统安全	ISS-11					√				
密码学概念	CRYPT-1	√	√						√	
分组密码	CRYPT-2		√							
流密码	CRYPT-3		√							
Hash 函数	CRYPT-4		√							
公钥密码	CRYPT-5		√							
密码协议	CRYPT-6		√	√						
数字签名	CRYPT-7		√							
认证	CRYPT-8		√	√						
密钥管理	CRYPT-9		√							
网络安全概念	NS-1	√		√						√
防火墙	NS-2			√						
入侵检测系统	NS-3			√						
虚拟专用网	NS-4			√						
网络安全协议	NS-5			√						
网络防护	NS-6			√	√					
Web 安全	NS-7			√		√	√			

续表

知识单元名称	知识单元编号	课程与编号								
		1	2	3	4	5	6	7	8	9
		信息安全导论 必修	应用密码学 必修	网络安全 必修	软件安全 必修	信息系统安全 必修	电子商务与电子政务安全 选修	信息犯罪与取证技术 选修	信息隐藏 选修	信息内容安全 选修
无线网络安全(选修)	NS-8			√						
信息内容安全概念	ICS-1	√		√		√		√	√	√
网络数据的获取	ICS-2			√				√		√
信息内容的分析与识别(选修)	ICS-3							√		√
信息内容的管控(选修)	ICS-4							√		√
多媒体信息隐藏(选修)	ICS-5							√	√	√
隐私保护(选修)	ICS-6	√		√					√	√

表 3-6　知识体系方案二的信息安全专业课程举例

序号	课程名称		必修知识单元	选修知识单元
1	基础类课程	信息安全导论	ISB-1，ISB-3，ISB-4，ISS-1，ISS-7，CRYPT-1，NS-1，ICS-1	ISS-8 ISS-9 ICS-6
2	专业类课程	应用密码学	ISB-1，ISB-2，CRYPT-1，CRYPT-2，CRYPT-3，CRYPT-4，CRYPT-5，CRYPT-6，CRYPT-7，CRYPT-8，CRYPT-9	

续表

序号	课程名称		必修知识单元	选修知识单元
3	专业类课程	网络安全	ISB-1,ISS-4, CRYPT-6,CRYPT-8,NS-1,NS-2,NS-3,NS-4,NS-5,NS-6,NS-7,ICS-1,ICS-2	NS-8 ICS-6
4		软件安全	ISS-7,NS-6	
5		信息系统安全	ISB-1,ISS-1,ISS-2,ISS-3,ISS-4,ISS-5,ISS-6,ISS-7,ISS-11,NS-7,ICS-1	
6		电子商务与电子政务安全(选修)	ISB-3,ISB-4,NS-7	ISS-8 ISS-9
7		信息犯罪与取证技术(选修)	ISB-3,ISB-4,ISS-5,ISS-6,ICS-1,ICS-2	ISS-10 ICS-3 ICS-4 ICS-5
8		信息隐藏(选修)	CRYPT-1,ICS-1	ICS-5 ICS-6
9		信息内容安全(选修)	ISB-1,ISB-3,ISB-4, NS-1, ICS-1,ICS-2	ICS-3 ICS-4 ICS-5 ICS-6 ISS-10

3.8　信息安全专业规范实践能力教学体系

实践能力体系要用实践教学体系来覆盖,通过实践教学体系的实施来培养和锻炼学生的实践能力。实践教学体系由多种实践教学环节组成。

本规范建议了4种实践教学环节:实验课,课间实验,课程设计,课外实习。

① 实验课：实验课是指作为一门课程，安排在课表中，有学分。

② 课间实验：课间实验是利用课外业余时间进行的一种实验，它不在课表中安排，也没有学分。

③ 课程设计：对于专业基础课和专业课，可以在课程的最后安排一段时间集中进行，是旨在巩固课程内容的配套实践活动。学生在老师的指导下进行一个与课程内容相关的实验，自主设计，自主完成。

④ 课外实习：主要是指学生利用课外时间，参加老师的科研项目组的科学研究工作，也可以是大学生业余科研活动。还可以是参加各种科研竞赛活动。

实际上，实践教学环节远不止以上 4 种，各学校完全可以根据自己的实际情况，设计出更多的实践教学环节。用这些实践教学环节去覆盖实践能力体系，都可以达到培养和提高学生实践能力的目的。

3.8.1 实践能力体系方案一的实践教学体系举例

实践能力体系方案一的实践教学体系举例如表 3-7 和表 3-8 所示。

表 3-7 实践能力体系方案一的实践环节与实践能力单元（能力点）的涵盖关系

实践能力单元（能力点）	实践能力单元（能力点）编号	实践环节与编号										
		1	2	3	4	5	6	7	8	9	10	11
		汇编语言实验 选修	C语言实验	Java程序设计实验 选修	网络程序设计实验	嵌入式系统实验	硬件实验	软件实验	网络安全实验	信息内容安全实验	课程设计	课外实践
汇编语言能力（选修）	SWSPA-1-1	√										
C 语言编程能力	SWSPA-1-2		√									

续表

实践能力单元(能力点)	实践能力单元(能力点)编号	实践环节与编号										
		1	2	3	4	5	6	7	8	9	10	11
		汇编语言实验 选修	C语言实验	Java程序设计实验 选修	网络程序设计实验	嵌入式系统实验	硬件实验	软件实验	网络安全实验	信息内容安全实验	课程设计	课外实践
Java语言编程能力(选修)	SWSPA-1-3			√								
Web编程能力(选修)	SWSPA-2-1				√							
Socket编程能力	SWSPA-2-2				√							
网络安全编程能力(选修)	SWSPA-2-3				√							
基础软件实践能力	SWSPA-3							√				
小型应用软件实践能力(选修)	SWSPA-4							√			√	√
恶意代码处理能力	SWSPA-5							√				
模拟电路与数字电子线路应用能力	HWSPA-1						√					
可编程集成电路应用能力(选修)	HWSPA-2					√	√					
嵌入式系统应用开发能力	HWSPA-3					√	√					
PC组配能力(选修)	HWSPA-4						√					
密码标准算法的软件实现与应用能力	CRYPTPA-1										√	
常用密码函数库及软件工具的应用能力(选修)	CRYPTPA-2										√	

续表

实践能力单元(能力点)	实践能力单元(能力点)编号	实践环节与编号										
		1	2	3	4	5	6	7	8	9	10	11
		汇编语言实验 选修	C语言实验	Java程序设计实验 选修	网络程序设计实验	嵌入式系统实验	硬件实验	软件实验	网络安全实验	信息内容安全实验	课程设计	课外实践
常用网络安全设备安装与配置能力	NSPA-1								√			
服务器环境搭建与安全配置能力(选修)	NSPA-2								√			
网络安全防护能力	NSPA-3								√			
小型网络安全整体解决方案设计能力	NSPA-4								√		√	
Web 安全实践能力	NSPA-5								√			
网络数据获取能力	ICSPA-1								√	√		
信息内容的分析与识别能力(选修)	ICSPA-2									√		
信息内容的管控能力(选修)	ICSPA-3									√		
多媒体信息隐藏实践能力(选修)	ICSPA-4									√		
隐私保护实践能力(选修)	ICSPA-5									√		
创新实践能力(选修)	CPA											√

表 3-8　实践能力体系方案一的实践教学能力教学体系举例

序号	环节	课程名	必修能力单元(能力点)	选修能力单元(能力点)
1	课间实验	汇编语言实验(选修)		SWSPA-1-1
2		C 语言实验	SWSPA-1-2	
3		Java 程序设计实验(选修)		SWSPA-1-3
4		网络程序设计实验	SWSPA-2-2	SWSPA-2-1 SWSPA-2-3
5	实验课程	嵌入式系统实验	HWSPA-3	HWSPA-2
6		硬件实验	HWSPA-1,SWSPA-3	HWSPA-2 HWSPA-4
7		软件实验	SWSPA-3,SWSPA-5	SWSPA-4
8		网络安全实验	NSPA-1,NSPA-3, NSPA-4,NSPA-5,ICSPA-1	NSPA-2
9		信息内容安全实验	ICSPA-1	ICSPA-2,ICSPA-3 ICSPA-4,ICSPA-5
10	课程设计	1. 各学校根据自己的特色,在部分专业课和专业基础课中设置课程设计。 2. 要求学生根据课程的内容,进行配套实践。 3. 要求覆盖课程的主要能力点。 4. 在本例中,如 SWSPA-4,CRYPTPA-1,CRYPTPA-2,NSPA-4等都可以通过课程设计的形式来进行实践教学。		
11	课外实践	1. 校外实习或院内课题组实习; 2. 参加各种信息安全竞赛	SWSPA-4,CPA(依托项目,结合实际项目研究或应用需求)	

3.8.2　实践能力体系方案二的实践教学体系举例

实践能力体系方案二的实践教学体系举例如表 3-9 和表 3-10 所示。

表 3-9　实践能力体系方案二的实践环节与实践能力单元（能力点）的涵盖关系

实践能力单元(能力点)	实践能力单元(能力点)编号	实践环节与编号												
		1	2	3	4	5	6	7	8	9	10	11	12	13
		汇编语言实验 选修	C语言实验	Java程序设计实验	网络程序设计实验	应用密码学实验	信息隐藏实验 选修	硬件实验	软件实验	嵌入式系统实验	网络安全实验	信息内容安全实验	课程设计	课外实践
汇编语言能力(选修)	SWSPA-1-1	√												
C 语言编程能力	SWSPA-1-2		√											
Java 语言编程能力	SWSPA-1-3			√										
Web 编程能力(选修)	SWSPA-2-1				√									
Socket 编程能力	SWSPA-2-2				√									
网络安全编程能力(选修)	SWSPA-2-3				√									
基础软件实践能力	SWSPA-3								√					
小型应用软件实践能力(选修)	SWSPA-4								√				√	√
恶意代码处理能力	SWSPA-5								√		√			
模拟电路与数字电路应用能力	HWSPA-1							√						

续表

实践能力单元(能力点)	实践能力单元(能力点)编号	实践环节与编号												
		1 汇编语言实验 选修	2 C语言实验	3 Java程序设计实验	4 网络程序设计实验	5 应用密码学实验	6 信息隐藏实验 选修	7 硬件实验	8 软件实验	9 嵌入式系统实验	10 网络安全实验	11 信息内容安全实验	12 课程设计	13 课外实践
可编程集成电路应用能力(选修)	HWSPA-2							√		√				
嵌入式系统应用开发能力	HWSPA-3							√		√				
PC组配能力(选修)	HWSPA-4							√						
密码标准算法的软件实现与应用能力	CRYPTPA-1					√							√	
常用密码函数库及软件工具应用能力	CRYPTPA-2					√							√	
常用网络安全设备安装与配置能力	NSPA-1										√			
服务器环境搭建与安全配置能力	NSPA-2										√			
网络安全防护能力	NSPA-3										√			
小型网络安全整体解决方案设计能力	NSPA-4										√		√	
Web安全实践能力	NSPA-5										√			
网络数据获取能力	ICSPA-1										√	√		

续表

实践能力单元(能力点)	实践能力单元(能力点)编号	实践环节与编号												
		1	2	3	4	5	6	7	8	9	10	11	12	13
		汇编语言实验 选修	C语言实验	Java程序设计实验	网络程序设计实验	应用密码学实验	信息隐藏实验 选修	硬件实验	软件实验	嵌入式系统实验	网络安全实验	信息内容安全实验	课程设计	课外实践
信息内容的分析与识别能力(选修)	ICSPA-2											√		
信息内容管控能力(选修)	ICSPA-3											√		
多媒体信息隐藏实践能力(选修)	ICSPA-4						√							
隐私保护能力(选修)	ICSPA-5											√		
创新实践能力(选修)	CPA													√

表 3-10　实践能力体系方案二的实践教学体系举例

序号	环节	课程名	必修能力单元(能力点)	选修能力单元(能力点)
1	课间实验	汇编语言实验		SWSPA-1-1
2		C 语言实验	SWSPA-1-2	
3		Java 程序设计实验	SWSPA-1-3	
4		网络程序设计实验	SWSPA-2-2	SWSPA-2-1 SWSPA-2-3
5		应用密码学实验	CRYPTPA-1,CRYPTPA-2	
6		信息隐藏实验		ICSPA-4

续表

序号	环节	课程名	必修能力单元(能力点)	选修能力单元(能力点)
7	实验课程	硬件实验	HWSPA-1,SWSPA-3	HWSPA-2 HWSPA-4
8		软件实验	SWSPA-3,SWSPA-5	SWSPA-4
9		嵌入式安全系统实验	HWSPA-3	HWSPA-2
10		网络安全实验	SWSPA-5,NSPA-1,NSPA-2,NSPA-3,NSPA-4,NSPA-5,ICSPA-1	
11		信息内容安全实验	ICSPA-1	ICSPA-2 ICSPA-3 ICSPA-5
12	课程设计	1. 各学校根据自己的特色,在部分专业课和专业基础课中设置课程设计。 2. 要求学生根据课程的内容,进行配套实践。 3. 要求覆盖课程的主要能力点。 4. 在本例中,如 SWSPA-4,CRYPTPA-1,CRYPTPA-2,NSPA-4 等都可以通过课程设计的形式来进行实践教学。		
13	课外实践	1. 校外实习或院内课题组实习; 2. 参加各种信息安全竞赛	SWSPA-4,CPA(依托项目,结合实际项目研究或应用需求)	

附录A

A.1　武汉大学信息安全专业的专业知识体系

武汉大学信息安全专业的专业知识体系采用规范中知识体系的方案一，并结合自己的实际情况进行了一定的扩充和调整，从而形成了武汉大学信息安全专业的专业知识体系。主要的扩充和调整如下：

(1) 覆盖规范知识体系方案一中的所有必修知识点；

(2) 适当增加了部分知识单元和知识点，以突出武汉大学的办学特色；

(3) 适当选择了规范知识体系方案一中的一些选修知识点，以突出武汉大学的办学特色；

(4) 对于规范知识体系方案一中的部分知识单元和知识点的学习目标，进行了一定的扩充和落实。

为了节省篇幅，这里没有给出武汉大学信息安全专业的专业知识体系的全文，仅给出了武汉大学信息安全专业课程体系对武汉大学信息安全专业的专业知识体系知识单元的覆盖关系表，如附表 A-1 所示。

附表 A-1　武汉大学课程体系对知识体系知识单元的覆盖关系表

知识单元名字	知识单元编号	课程																
		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
		信息安全导论	信息安全数学基础	密码学	网络安全	软件安全	操作系统原理及安全	数据库原理及安全	嵌入式系统安全	信息内容安全	信息隐藏	主流操作系统安全技术	电子政务与电子商务安全	信息系统安全导论	计算机取证	无线网络安全	可信计算技术	程序分析
		选修								选修	选修	选修	选修	选修	选修	选修	选修	选修
信息安全概念	ISB-1	√		√	√	√		√						√				
数论	ISB-2-1		√															
代数结构	ISB-2-2		√															
组合数学（选修）	ISB-2-3		√															
计算复杂性（选修）	ISB-2-7		√															
信息安全法律基础	ISB-3	√								√			√		√			
信息安全管理基础	ISB-4	√								√			√					
信息系统安全概念	ISS-1	√					√	√	√					√			√	
信息系统设备安全	ISS-2								√					√				
信息系统可靠性技术	ISS-3								√					√				
访问控制	ISS-4						√	√				√		√				
操作系统安全	ISS-5						√		√			√		√				
数据库安全	ISS-6							√						√				

续表

知识单元名字	知识单元编号	课程																
		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
		信息安全导论 选修	信息安全数学基础	密码学	网络安全	软件安全	操作系统原理及安全	数据库原理及安全	嵌入式系统安全	信息内容安全 选修	信息隐藏 选修	主流操作系统安全技术 选修	电子政务与电子商务安全 选修	信息系统安全导论 选修	计算机取证 选修	无线网络安全 选修	可信计算技术 选修	程序分析 选修
软件安全	ISS-7	√				√								√				√
电子商务安全（选修）	ISS-8	√											√					
电子政务安全（选修）	ISS-9	√											√					
数字取证技术（选修）	ISS-10									√					√			
嵌入式系统安全	ISS-11								√					√				
可信计算（选修）	*ISS-12*													√			√	
密码学概念	CRYPT-1	√	√	√							√							
分组密码	CRYPT-2			√														
流密码	CRYPT-3			√														
Hash 函数	CRYPT-4			√														
公钥密码	CRYPT-5			√														
密码协议	CRYPT-6			√	√											√		

续表

知识单元名字	知识单元编号	课程																
		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
		信息安全导论 选修	信息安全数学基础	密码学	网络安全	软件安全	操作系统原理及安全	数据库原理及安全	嵌入式系统安全	信息内容安全 选修	信息隐藏 选修	主流操作系统安全技术 选修	电子政务与电子商务安全 选修	信息系统安全导论 选修	计算机取证 选修	无线网络安全 选修	可信计算技术 选修	程序分析 选修
数字签名	CRYPT-7			√														
认证	CRYPT-8			√	√													
密钥管理	CRYPT-9			√														
密码应用	*CRYPT-10*			√					√									
网络安全概念	NS-1	√			√	√				√								
防火墙	NS-2				√													
入侵检测系统	NS-3				√													
虚拟专用网	NS-4				√													
网络安全协议	NS-5				√											√		
网络防护	NS-6				√									√		√		
Web 安全	NS-7				√								√	√				
无线网络安全（选修）	NS-8				√											√		
信息内容安全概念	ICS-1	√			√					√	√							

续表

知识单元名字	知识单元编号	课程																
		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
		信息安全导论 选修	信息安全数学基础	密码学	网络安全	软件安全	操作系统原理及安全	数据库原理及安全	嵌入式系统安全	信息内容安全 选修	信息隐藏 选修	主流操作系统安全技术 选修	电子政务与电子商务安全 选修	信息系统安全导论 选修	计算机取证 选修	无线网络安全 选修	可信计算技术 选修	程序分析 选修
网络数据的获取	ICS-2				√					√						√		
信息内容的分析与识别(选修)	ICS-3									√								
信息内容的管控(选修)	ICS-4									√								
多媒体信息隐藏(选修)	ICS-5									√	√							
隐私保护(选修)	ICS-6	√			√					√	√							
多媒体加密技术(选修)	*ICS-7*									√								
多媒体内容取证(选修)	*ICS-8*									√					√			

注 1：表中的斜体部分表示该知识单元是武汉大学扩充的知识单元；

注 2：从表中看不出武汉大学对部分知识点和对学习目标要求的扩充，可以在武汉大学信息安全专业的专业知识体系中看到。

A.2　武汉大学信息安全专业实践能力体系

武汉大学信息安全专业的实践能力体系采用规范中实践能力体系的方案一，并结合自己的实际情况进行了一定的扩充和调整，从而形成了武汉大学信息安全专业的实践能力体系。主要的扩充和调整如下：

（1）覆盖规范实践能力体系方案一中的所有必修实践能力点；

（2）适当增加了部分实践能力单元和实践能力点，以突出武汉大学的办学特色；

（3）全部选用了规范实践能力体系方案一中的选修实践能力点，并将其中许多选修实践能力点改变为必修实践能力点，以突出武汉大学的办学特色；

（4）对于规范实践能力体系方案一中的部分实践能力单元和实践能力点的学习目标，进行了一定的扩充和落实。

为了节省篇幅，这里没有给出武汉大学信息安全专业实践能力体系的全文，仅给出了武汉大学信息安全专业实践教学体系对武汉大学信息安全专业实践能力体系实践能力单元的覆盖关系表，如附表 A-2 所示。

附表 A-2　武汉大学实践教学体系对实践能力体系实践能力单元的覆盖关系表

实践能力单元（能力点）	编号	实践教学环节与编号																	
		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
		程序设计综合训练	C程序设计实验	操作系统及安全课程设计	计算机组成原理实验	数据库原理及安全实验	计算机网络应用设计	电路与电子技术实验	数字逻辑实验	EDA及应用实验	嵌入式系统安全实验	软件安全实验	密码学课程设计	网络安全实验	信息内容安全实验	信息隐藏实验	网络程序设计实验	微机系统与接口技术实验	软件工程实验
		必修	必修	必修	必修	必修	必修	必修	必修	选修	必修	必修	必修	必修	选修	选修	选修	选修	选修
汇编语言能力（选修）	SWSPA-1-1	√																√	
C语言编程能力	SWSPA-1-2	√	√																
Java语言编程能力（选修）	SWSPA-1-3	√																	
Web编程能力（选修）	SWSPA-2-1																√		
Socket编程能力	SWSPA-2-2						√							√			√		
网络安全编程能力	SWSPA-2-3											√					√		
基础软件实践能力	SWSPA-3			√		√													
小型应用软件实践能力（选修）	SWSPA-4																		√
恶意代码处理能力	SWSPA-5											√							

续表

实践能力单元（能力点）	编号	实践教学环节与编号																	
		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
		程序设计综合训练	C程序设计实验	操作系统及安全课程设计	计算机组成原理实验	数据库原理及安全实验	计算机网络应用设计	电路与电子技术实验	数字逻辑实验	EDA及应用实验	嵌入式系统安全实验	软件安全实验	密码学课程设计	网络安全实验	信息内容安全实验	信息隐藏实验	网络程序设计实验	微机系统与接口技术实验	软件工程实验
		必修	必修	必修	必修	必修	必修	必修	必修	选修	必修	必修	必修	必修	选修	选修	选修	选修	选修
模拟电子线路应用能力	*HWSPA-1-whu*							√											
数字电子线路应用能力	HWSPA-1								√										
可编程集成电路应用能力	HWSPA-2									√	√		√						
嵌入式系统应用开发能力	HWSPA-3										√								
PC组配能力（选修）	HWSPA-4																	√	
计算机硬件组成部件实现能力	*HWSPA-4-whu*				√													√	
密码标准算法的软件实现与应用能力	CRYPTPA-1												√						
常用密码函数库及软件工具的应用能力	*CRYPTPA-2*												√						

续表

实践能力单元（能力点）	编号	实践教学环节与编号																	
		1 程序设计综合训练 必修	2 C程序设计实验 必修	3 操作系统及安全课程设计 必修	4 计算机组成原理实验 必修	5 数据库原理及安全实验 必修	6 计算机网络应用设计 必修	7 电路与电子技术实验 必修	8 数字逻辑实验 必修	9 EDA及应用实验 选修	10 嵌入式系统安全实验 必修	11 软件安全实验 必修	12 密码学课程设计 必修	13 网络安全实验 必修	14 信息内容安全实验 选修	15 信息隐藏实验 选修	16 网络程序设计实验 选修	17 微机系统与接口技术实验 选修	18 软件工程实验 选修
常用网络安全设备安装与配置能力	NSPA-1													√					
服务器环境搭建与安全配置能力	NSPA-2													√					
网络防护能力	NSPA-3													√					
小型网络安全整体解决方案设计能力	NSPA-4													√					
Web 安全实践能力	NSPA-5													√					
网络应用设计能力	*NSPA-6-whu*						√												
网络数据获取能力	ICSPA-1													√	√				
信息内容的分析与识别能力（选修）	ICSPA-2														√				

续表

实践能力单元（能力点）	编号	实践教学环节与编号																	
		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
		程序设计综合训练	C程序设计实验	操作系统及安全课程设计	计算机组成原理实验	数据库原理及安全实验	计算机网络应用设计	电路与电子技术实验	数字逻辑实验	EDA及应用实验	嵌入式系统安全实验	软件安全实验	密码学课程设计	网络安全实验	信息内容安全实验	信息隐藏实验	网络程序设计实验	微机系统与接口技术实验	软件工程实验
		必修	必修	必修	必修	必修	必修	必修	必修	选修	必修	必修	必修	必修	选修	选修	选修	选修	选修
信息内容的管控能力（选修）	ICSPA-3														√				
多媒体信息隐藏实践能力（选修）	ICSPA-4															√			
隐私保护能力（选修）	ICSPA-5														√	√			
多媒体内容加密技术实践能力（选修）	*ICSPA-6-whu*														√				
多媒体内容取证实践能力（选修）	*ICSPA-7-whu*														√				
创新实践能力（选修）	CPA											√	√	√					√

注 1：表中的斜体部分表示该实践能力单元是武汉大学扩充的实践能力单元；

注 2：从表中看不出武汉大学对部分实践能力点和对学习目标要求的扩充，可以在武汉大学信息安全专业实践能力体系中看到。

A.3 武汉大学信息安全本科专业人才培养方案

一、学院简介

武汉大学计算机学院前身可追溯到1978年由原武汉大学建立的计算机科学系，是全国最早建立的计算机科学系之一。

武汉大学计算机学院现有4个系：计算机科学系、计算机工程系、计算机应用系、信息安全系；一个实验中心；三个研究所：计算机软件研究所、计算机应用研究所、计算机网络研究所；三个本科专业：计算机科学与技术专业、信息安全专业、物联网工程专业；八个硕士点：计算机系统结构、计算机软件与理论、计算机应用技术、信息安全、软件工程、数字影视技术、通信与信息系统、模式识别与智能系统；六个博士点：计算机系统结构、计算机软件与理论、计算机应用技术、信息安全、软件工程、通信与信息系统。有计算机科学与技术一级学科博士授权点，计算机科学与技术博士后科研流动站。计算机软件与理论是国家重点学科，计算机应用技术是湖北省重点学科。计算机科学与技术、信息安全两个本科专业是国家特色专业，实验中心是湖北省实验教学示范中心。学院学科构架完整，科研平台齐全，包括空天信息安全与可信计算教育部重点实验室、软件工程国家重点实验室、国家多媒体软件工程技术研究中心、国家信息安全产品测评认证中心互操作性测评中心、国家Linux技术培训与推广中心、湖北省多媒体网络通信工程重点实验室等科学研究基地。

学院现有专任教师199人，其中教授50人，副教授89人。雄厚的师资力量、先进的教学设施，使武汉大学计算机学院在信息安全、智能计算、软件工程、多媒体技术、网络与分布处理、生物信息、建模与仿真、安防数字化智能化等方向的研究具有较强的科研和教学力量。

二、培养方案主要内容

（一）专业代码、名称

专业代码：080904K

专业名称：信息安全 Information Security

（二）专业培养目标

培养德、智、体等全面发展，掌握自然科学、人文科学和信息科学基础知识，系统掌握信息安全领域的基本理论、基本技术和应用知识，具备信息安全科学研究、技术开发和应用服务工作能力的信息安全专业人才；培养的毕业生能够从事计算机、通信、电子信息、电子商务、电子金融、电子政务、军事、公安等领域的信息安全研究、应用、开发和管理等方面的工作。

（三）专业特色和培养要求

2001 年，经教育部批准武汉大学创建了我国第一个信息安全本科专业，目前已具备信息安全硕士点、博士点和博士后产业基地，形成了信息安全人才培养的完整体系。2007 年，武汉大学的信息安全专业获得“湖北省品牌专业”称号，2008 年获得“国家特色专业建设点”、“空天信息安全与可信计算教育部重点实验室”。武汉大学在密码学、信息系统安全、网络安全和信息内容安全等领域都开展了广泛而深入的科学研究，取得了一批在国内外有影响的科研成果。目前，武汉大学在信息安全学科领域已形成了自己的特色和优势，已成为我国信息安全人才培养和科学研究的重要基地。所培养的毕业生受到社会的广泛好评。

信息安全学科是综合计算机、电子、通信、数学、物理、生物、管理、法律和教育等学科发展演绎而形成的交叉学科。信息安全学科是研究信息的获取、存储、传输和处理中的安全保障问题的一门新兴学科。要求学生掌握信息安全基础理论，具备信息安全科学研究、技术开发和应用服务工作的能力；能熟练掌握一门外国语，阅读本专业的外文资料。

（四）学制和学分要求

学制：四年，其中前三学年在校内进行课程学习，第四学年到单位实习并完成毕业论文，推荐或考上研究生的同学，直接进入导师课题组实习。

学分要求：毕业生毕业时必须修满 150 学分，其中通识教育课 60 学分（其中通识教育必修课 26 学分），专业必修课 47.5 学分，集中实践教学环

节必修课 9.5 学分，专业选修课最低 27 学分，毕业论文 6 学分。

（五）学位授予

授予工学学士学位。

（六）专业主干（核心）课程、双语（全英文）课程、特色课程

学科基础（平台）课程：数字逻辑、计算机组成原理、离散数学、数据结构、高级语言程序设计、操作系统及安全、数据库原理及安全、计算机网络及通信原理、信息安全数学基础、密码学、网络安全。

其他主干课程：通信原理、嵌入式系统安全、软件安全、网络管理、信息隐藏、信息系统安全导论、信息内容安全、电子商务与电子政务安全、网络程序设计、可信计算技术，其中可信计算技术为双语课程。

（七）主要实验和实践性教学要求

包括电路与电子技术实验、数字逻辑实验、计算机组成原理实验、操作系统及安全课程设计、程序设计综合训练、计算机网络应用设计、密码学课程设计、软件安全实验、网络安全实验、嵌入式系统安全实验等。

实践性教学环节主要有上机实习和实验两种类型，采用课间实验与集中实验相结合的方法进行安排。其中，课间实验与相应课程同步进行。集中实验一般在相应课程结束后集中进行，以综合性、设计型为主，旨在锻炼综合应用知识、解决实际问题的能力。每个学生必须从二年级开始参加一个兴趣小组，承担相应的课外研究、开发工作。推荐免试攻读硕士学位的学生直接进入到导师的课题组，提前开始研究生阶段的学习和研发工作；对准备就业的学生，到用人单位或实习基地实习锻炼。

（八）毕业生条件及其他必要的说明

毕业生毕业时必须修满 150 学分并完成兴趣小组分配的任务方可颁发本科毕业文凭，成绩符合武汉大学学位授予条件且获得国家英语四级证书者，才能获得工学学士学位证书。

三、专业教学计划样表

计算机学院 信息安全专业教学计划表

课程类别		课程编号	课程名称	学分数	总学时	学时类型					各学期学时学分分配								开课学院
						讲课	习题课	实验	实践	上机	1	2	3	4	5	6	7	8	
通识课程	必修	0100002	毛泽东思想和中国特色社会主义理论体系概论	3	54						学生自由选择修习时间								政
		0300182	马克思主义基本原理	3	54														政
		0300181	思想道德修养和法律基础	3	54														政
		0600120	中国近现代史纲要	3	54														政
			形势与政策	2	36						学生自由选择修习时间，不计入学位学分								政
			国情教育与社会实践	2	36														政
			英语								选择下述综合英语1、2、3、4这4个类别之一，计算机学院学生毕业至少需修够9学分								英
			综合英语1起点	12	216						A1＋A2＋A3＋A4，根据英语分级考试成绩选择综合英语1、2、3、4起点修习，4个类别选择1类修习即可，所修类别必须完整修习								英

续表

课程类别		课程编号	课程名称	学分数	总学时	学时类型					各学期学时学分分配								开课学院
						讲课	习题课	实验	实践	上机	1	2	3	4	5	6	7	8	
通识课程	必修		综合英语2起点	11	198						A2＋A3＋A4＋Bn								英
			综合英语3起点	10	180						A3＋A4＋Bn＋Bn								英
			综合英语4起点	9	162						A4＋Bn＋Bn＋Bn								英
		1200001	体育	4	144						按项目学生自由选择修习时间								体
		1200005	军事理论	1	18						学生自由选择修习时间，18学时的实践内容归入军事训练								军
	选修		*交流与写作类*	2							至少2学分				其中必选类课程是此专业学生大学期间必须选修的，其余课程可自由选修全校各类通识选修课程达到基本学分要求。网页设计与制作为计算机学院学生推荐选修				
			数学与推理类	16							包括下列4门								
		0700005	高等数学B1	5	90						数学与推理类必选								数
		0700005	高等数学B2	5	90						数学与推理类必选								数
		0700010	线性代数B	3	54						数学与推理类必选								数
		0700001	概率论与数理统计B	3	54						数学与推理类必选								数
			人文与社会类	4							至少4学分								
			自然与工程类	6							至少6学分								

续表

课程类别		课程编号	课程名称	学分数	总学时	学时类型					各学期学时学分分配								开课学院
						讲课	习题课	实验	实践	上机	1	2	3	4	5	6	7	8	
通识课程	选修	0800497	计算机导论	3	36			36			计算机专业与工程类必选								计
			网络安全	3	54	54					信息安全专业与工程类必选（建议完成计算机网络课程学习以后修）								计
			艺术与欣赏类	2							至少 2 学分								
			中国与全球类	2							至少 2 学分								
			研究与领导类	2							至少 2 学分								
专业课程	必修	0800498	电路与电子技术	4	72	72					4								计
		0800499	数字逻辑	3	54	54						3							计
		0800500	高级语言程序设计	4	90	54				36		4							计
		0800052	计算机组成原理	4	72	72							4						计
		1100145	离散数学	3	54	54							3						计

续表

课程类别			课程编号	课程名称	学分数	总学时	学时类型					各学期学时学分分配								开课学院
							讲课	习题课	实验	实践	上机	1	2	3	4	5	6	7	8	
专业课程	必修		0800109	数据结构	4	72	72							4						计
专业课程	必修		0800503	信息安全数学基础	4	72	72								4					计
专业课程	必修		0802047	操作系统原理及安全	4	72	72								4					计
专业课程	必修			数据库原理及安全	3.5	63	63								3.5					计
专业课程	必修		0800069	通信原理	2	36	36								2					计
专业课程	必修		0800074	计算机网络	3	54	54									3				计
专业课程	必修		0800507	密码学	3	54	54									3				计
专业课程	必修		0802048	软件安全	3	54	54										3			计
专业课程	必修			嵌入式系统安全	3	54	54											3		计
专业课程	选修	基础		信息安全导论	1	18	18					1								计
专业课程	选修	基础	0800521	算法设计与分析	3	54	54										3			计
专业课程	选修	基础	0800522	编译原理	3	54	54									3				计
专业课程	选修	基础	0800523	软件工程	3	72	36				36					3				计

续表

课程类别			课程编号	课程名称	学分数	总学时	学时类型					各学期学时学分分配								开课学院
							讲课	习题课	实验	实践	上机	1	2	3	4	5	6	7	8	
专业课程	选修	基础	0800506	微机系统与接口技术	3	63	45				18						3			计
			0802225	EDA 及应用	3	72	36				36				3					计
				计算机创新素质训练	2	36	36										2			计
		系统安全		主流操作系统安全技术	2	36	36									2				计
				信息系统安全导论	2	36	36								2					计
				计算机取证	2	36	36											2		计
				云计算及安全	2	36	36											2		计
				程序分析	2	36	36											2		计
				可信计算技术	3	72	36				36						3			计
		网络安全	0800508	网络程序设计	3	72	36				36						3			计
			0800519	网络管理	2	36	36										2			计
				无线网络安全	2	36	36											2		计
			0802053	电子商务与电子政务安全	3	54	54											3		计
			0802205	物联网工程导论	1	18	18					1								计

续表

课程类别			课程编号	课程名称	学分数	总学时	学时类型					各学期学时学分分配								开课学院
							讲课	习题课	实验	实践	上机	1	2	3	4	5	6	7	8	
专业课程	选修	内容安全	0800067	数字信号处理	2	36	36								2					计
			0800773	多媒体技术	3	54	54									3				计
			0800520	模式识别	2	36	36										2			计
			0800517	信息隐藏技术	3	72	36		36							3				计
			0802050	信息内容安全	3	72	36		36								3			计
	实践教学			生产劳动		2 周														计
			1300154	电路与电子技术试验	0.5	1 周						0.5								计
			1300155	数字逻辑实验	1	2 周			1 周	1 周				1						计
			1300156	计算机组成原理实验	1	2 周			1 周	1 周					1					计
			1300723	密码学课程设计	0.5	1 周			1 周						0.5					计
				操作系统及安全设计	1	2 周			2 周							1				计
				数据库系统安全实验	0.5	1 周			1 周							0.5				
				网络安全实验	1	2 周			2 周								1			

续表

课程类别		课程编号	课程名称	学分数	总学时	学时类型					各学期学时学分分配								开课学院
						讲课	习题课	实验	实践	上机	1	2	3	4	5	6	7	8	
专业课程	实践教学	1300724	软件安全实验	1	2 周			2 周								1			计
		1300159	计算机网络应用设计	1	2 周											1			计
		1300505	程序设计训练	1	2 周												1		计
			嵌入式系统安全实验	1	2 周			2 周									1		计
	毕业论文或设计必修学分			6	2 周													6	计
任意选修课程	任意选修课程是作为专业补充或个人兴趣爱好而由学生自主选择的课程。鼓励学生跨院(系)、跨专业选修课程,学院(系)对学生的选课给予必要的指导。具体学分数以满足各专业毕业最低总学分要求为准																		
毕业应取得总学分 150 学分				通识课程学分 60,占总学分 40% 其中必修课程学分 26,占通识教育学分 43.3% 选修课程学分 34,占通识教育学分 56.7%															
				专业课程学分 90,占总学分 58% 其中必修课程学分 47.5,占专业教育学分 52.8% 选修课程学分 27,占专业教育学分 30% 实践教学学分 9.5,占专业教育学分 10.6% 毕业论文或设计学分 6,占专业教育学分 6.6%															
				任意选修课程学分 0,占总学分 0%															